Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/004202

International filing date: 10 March 2005 (10.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-106339
Filing date: 31 March 2004 (31.03.2004)

Date of receipt at the International Bureau: 12 May 2005 (12.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2005/004202

日本国特許庁
JAPAN PATENT OFFICE

14. 3. 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年　３月３１日
出願番号 Application Number:	特願２００４－１０６３３９
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－１０６３３９
出願人 Applicant(s):	松下電器産業株式会社

２００５年　４月２１日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０３６５９７

【書類名】　特許願
【整理番号】　2048160113
【あて先】　特許庁長官殿
【国際特許分類】　H04N　7/16
G06F　7/14
G06F 12/00
G06F 15/177　682
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　東　吾紀男
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　岡本　隆一
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　村上　弘規
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　徳田　克己
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100109210
【弁理士】
【氏名又は名称】　新居　広守
【手数料の表示】
【予納台帳番号】　049515
【納付金額】　21,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0213583

【書類名】特許請求の範囲
【請求項１】
ユーザに対して、コンテンツの利用許諾を与えるためのライセンスを配信する送出装置と、前記ライセンスを取得し、前記ライセンスに基づきコンテンツをセキュアに利用する端末装置と、から構成されるデジタル権利管理システムであって、
前記送出装置は、前記ライセンスを生成するライセンス生成手段と、
前記ライセンスに、ＩＤを付与するライセンスＩＤ付与手段と、
前記ライセンスに、前記ライセンスの取得が可能な期限を示すライセンス取得期限を付与するライセンス取得期限付与手段と、
前記ライセンスを前記端末装置に送出するライセンス送出手段と、
を備え、
前記端末装置は、
前記ライセンスを取得するライセンス取得手段と、
少なくとも、前記ライセンスに付加された前記ライセンスＩＤと、前記ライセンス取得期限と、を含むライセンス取得履歴を記録するライセンス取得履歴記録手段と、
前記ライセンスの取得時に、取得する前記ライセンスのライセンスＩＤと同一のライセンスＩＤが、前記ライセンス取得履歴記録手段が保持する前記ライセンス取得履歴に存在する場合に、前記ライセンスの取得を抑制するライセンス取得抑制手段と、
を備え、
前記ライセンス取得履歴記録手段は、少なくとも前記ライセンス取得期限までは、前記ライセンスＩＤと前記ライセンス取得期限からなる前記ライセンス取得履歴を保持する
ことを特徴とするデジタル権利管理システム。
【請求項２】
前記端末装置は、さらに、前記ライセンスのフォーマットを変換するライセンス変換手段を備え、
前記ライセンス変換手段は、前記ライセンスの取得時に、前記ライセンスのフォーマットを変換し、前記ライセンスのフォーマットを変換した履歴を、前記ライセンス取得履歴として前記ライセンス取得履歴記録手段に送信する
ことを特徴とする請求項１記載のデジタル権利管理システム。
【請求項３】
前記送出装置は、さらに、前記ライセンスを暗号化して暗号化ライセンスを生成するライセンス暗号化手段を備え、
前記端末装置は、さらに、前記暗号化ライセンスを復号して復号済みライセンスを生成するライセンス復号手段と、
前記復号済みライセンスを再暗号化するライセンス再暗号化手段と
を備え、
前記ライセンス再暗号化手段は、前記送出装置が送出する前記暗号化ライセンスとは異なる暗号鍵を用いて、前記復号済みライセンスを再暗号化することにより、前記ライセンスを前記端末装置にバインドする
ことを特徴とする請求項１記載のデジタル権利管理システム。
【請求項４】
前記ライセンスは、デジタル放送のＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ）あるいはＡＣＩ（Ａｃｃｏｕｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ）あるいはＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｍｅｓｓａｇｅ）のいずれかに設定される、または、前記ライセンスは、ＥＣＭあるいはＡＣＩあるいはＥＭＭのいずれかそのものである
ことを特徴とする請求項１記載のデジタル権利管理システム。
【請求項５】
前記ライセンス取得期限は、前記ライセンスの有効期限である
ことを特徴とする請求項１または請求項４記載のデジタル権利管理システム。

【請求項６】
前記ライセンス取得期限は、前記ライセンスの有効期限とは別に設定される
ことを特徴とする請求項１または請求項４記載のデジタル権利管理システム。
【請求項７】
前記送出装置は、さらに、前記ライセンスに前記ライセンス取得期限を付与するか否かを決定する前記ライセンス取得期限付与決定手段を備え、
前記ライセンス取得履歴記録手段は、前記ライセンス取得期限付与決定手段が前記ライセンスに前記ライセンス取得期限を設定しない場合には、前記ライセンス取得履歴の前記ライセンス取得期限を生成する
ことを特徴とする請求項１記載のデジタル権利管理システム。
【請求項８】
前記送出装置は、さらに、前記ライセンスにサービス種別を設定するサービス種別設定手段を備え、
前記ライセンス取得履歴記録手段は、前記ライセンスに設定された前記サービス種別に基づき、ライセンス取得履歴を記録するか否かを決定する
ことを特徴とする請求項１記載のデジタル権利管理システム。
【請求項９】
前記ライセンス取得履歴記録手段は、前記サービス種別がデジタル放送におけるフラット／ティア契約であるライセンスのみを、ライセンス取得履歴として記録する
ことを特徴とする請求項８記載のデジタル権利管理システム。
【請求項１０】
前記送出装置は、さらに、前記ライセンスにサービス種別を設定するサービス種別設定手段を備え、
前記ライセンス取得履歴記録手段は、さらに、前記サービス種別を前記ライセンス取得履歴として記録する
ことを特徴とする請求項１記載のデジタル権利管理システム。
【請求項１１】
前記送出装置は、さらに、前記ライセンスにライセンス取得条件を付与するライセンス取得条件付与手段を備え、
前記ライセンス取得抑制手段は、前記ライセンスに付与された前記ライセンス取得条件に基づき、前記ライセンスの取得を制御する
ことを特徴とする請求項１記載のデジタル権利管理システム。
【請求項１２】
前記端末装置は、さらに、ハードウェア的に耐タンパ化されたセキュリティモジュールを備え、
前記セキュリティモジュールが、前記ライセンス取得履歴記録手段および前記ライセンス取得抑制手段および前記ライセンス取得手段の少なくとも１つを備える
ことを特徴とする請求項１記載のデジタル権利管理システム。
【請求項１３】
前記端末装置は、さらに、少なくとも前記ライセンス取得履歴の一部を前記端末装置に蓄積するライセンス取得履歴蓄積手段を備え、
前記セキュリティモジュールは、さらに、少なくとも前記ライセンス取得履歴蓄積手段に蓄積した前記ライセンス取得履歴を含むデータのハッシュ値を保持するハッシュ値保持手段を備える
ことを特徴とする請求項１２記載のデジタル権利管理システム。
【請求項１４】
前記端末装置は、前記端末装置を特定可能な端末装置ＩＤを保持する第１の端末装置ＩＤ保持手段を備え、
前記セキュリティモジュールは、前記端末装置ＩＤを保持する第２の端末装置ＩＤ保持手段を備え、

前記第２の端末装置ＩＤ保持手段は、前記ライセンス取得手段が最初に前記ライセンスを取得した時点で挿入されている前記端末装置の前記第１の端末装置ＩＤ保持手段から取得した前記端末装置ＩＤを保持し、

前記ライセンス取得抑制手段は、前記ライセンスを取得する場合に、前記第１の端末装置ＩＤ保持手段から取得した端末装置ＩＤと、前記第２の端末装置ＩＤ保持手段に保持する端末装置ＩＤとを比較し、一致しない場合には、前記端末装置でのさらなる前記ライセンスの取得を抑制する

ことを特徴とする請求項１２記載のデジタル権利管理システム。

【請求項１５】

前記端末装置は、前記端末装置を特定可能な端末装置ＩＤを保持する第１の端末装置ＩＤ保持手段を備え、

前記セキュリティモジュールは、前記ライセンス取得履歴蓄積手段に前記ライセンス取得履歴を蓄積した場合に、前記ライセンス取得履歴を蓄積した前記端末装置の第１の端末装置ＩＤ保持手段から取得する前記端末装置ＩＤを保持する第２の端末装置ＩＤ保持手段を備え、

前記ライセンス取得抑制手段は、前記ライセンスを取得する場合に、前記第１の端末装置ＩＤ保持手段から取得した端末装置ＩＤと、前記第２の端末装置ＩＤ保持手段に保持する端末装置ＩＤとを比較し、一致しない場合には、前記端末装置でのさらなる前記ライセンスの取得を抑制する

ことを特徴とする請求項１３記載のデジタル権利管理システム。

【請求項１６】

前記端末装置は、さらに、ユーザに警告などのメッセージを提示するためのメッセージ提示手段を備え、

前記メッセージ提示手段は、前記ライセンス取得抑制手段が前記ライセンスの取得を抑制した場合に、少なくとも、前記ライセンスの取得ができない旨、あるいは、前記ライセンスの取得ができない理由をメッセージとしてユーザに提示する

ことを特徴とする請求項１記載のデジタル権利管理システム。

【書類名】明細書
【発明の名称】デジタル権利管理システム
【技術分野】
【０００１】
本発明は、デジタル放送、インターネットなどで配信される映像、音楽などのデジタルコンテンツの利用権利を管理し、ユーザが利用権利に基づき端末装置でデジタルコンテンツを利用するシステムに関し、特に、端末装置におけるデジタルコンテンツの利用権利の取得を、事業者の意図に従って確実に制御することが可能なシステムに関する。
【背景技術】
【０００２】
近年、音楽、映像などのデジタルコンテンツ（以下、コンテンツと記述）を、デジタル放送、デジタルＣＡＴＶ（Ｃａｂｌｅ　Ｔｅｌｅｖｉｓｉｏｎ）、インターネットなどを通じて、放送局から端末装置に配信し、端末装置においてコンテンツを利用することが可能なコンテンツ配信サービスが実用化の段階を迎えている。このコンテンツ配信サービスでは、コンテンツの著作権を保護し、悪意あるユーザなどによるコンテンツの不正利用を防止するため、著作権保護技術が用いられるのが一般的である。著作権保護技術とは、具体的には、暗号技術や認証技術などを用いて、ユーザがコンテンツを再生したり、記録メディアにコピーしたりといったようなコンテンツの利用を、セキュアに制御する技術である。著作権保護技術を用いることにより、放送局などのコンテンツプロバイダ、サービスプロバイダが、端末装置におけるユーザのコンテンツ利用をセキュアに制御することが可能となる。
【０００３】
ところで、近年、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）などの大容量蓄積手段を有する端末装置において、配信されたコンテンツを一旦端末装置に蓄積し、ユーザが好きなときに蓄積されたコンテンツを視聴するという、ユーザ利便性の高い利用形態が検討されている。日本におけるデジタル放送の規格化団体であるＡＲＩＢ（Ａｓｓｏｃｉａｔｉｏｎ　ｏｆ　Ｒａｄｉｏ　Ｉｎｄｕｓｔｒｉｅｓ　ａｎｄ　Ｂｕｓｉｎｅｓｓｅｓ）においては、大容量蓄積機能を活用するデジタル放送方式として、サーバ型放送方式が規格化されており、特にコンテンツの蓄積時における再生を限定するため方式として、限定再生方式が策定されている。なお、サーバ型放送方式における限定再生方式については、ＡＲＩＢ　ＳＴＤ－Ｂ２５　４．１版が詳しい。
【０００４】
このような蓄積機能を有する端末装置においては、コンテンツとともに、コンテンツの利用権利であるライセンスも端末装置に蓄積されるため、ライセンスを自由に複製することが可能である。その結果、同一のコンテンツについて複数のライセンスが無制限に取得できてしまう可能性が生ずる。もちろん、通常ライセンスは暗号化が施された状態で配信されるため、どのユーザであっても自由に利用できるわけではないが、少なくとも放送局との視聴契約を行ったユーザについては、特に月ぎめ契約（サブスクリプション）の場合などは、ライセンスを無制限に取得することが容易に可能となる。
【０００５】
特許文献１では、このような課題と類似の課題を解決するデジタル権利管理システムとして、記録媒体に書き出すコンテンツの数を制限するため、記録媒体に書き出すコンテンツＩＤをリストで管理する手法が開示されている。また、この手法では、コンテンツＩＤを記載したリストサイズの無制限な増加を防止するため、リストサイズの上限も管理しており、リストのサイズが上限に達した場合には、リストへの登録日時の古いレコードの順にコンテンツＩＤを削除するようになっている。
【特許文献１】特開２００４－５５２６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】

しかしながら、従来のデジタル権利管理システムでは、登録日時の古い順に、リストからレコードを削除する方式であるので、リストへのライセンスＩＤの登録・削除の繰り返しにより、結果的に複数の同一ライセンスを無制限に不正に取得されてしまう可能性があり、ユーザの取得可能なライセンス数を制限したいという事業者の権利を十分に保護することができない、という課題があった。

【０００７】

本発明は、こうした従来の問題点を解決するものであり、デジタル放送などにおいてライセンスを配信する場合に、ユーザによる無制限なライセンス取得を防止するとともに、リストのサイズの増大を防止することが可能なデジタル権利管理システムを提供することを目的としている。

【課題を解決するための手段】

【０００８】

上記目的を達成するために、本発明に関わるデジタル権利管理システムは、ユーザに対して、コンテンツの利用許諾を与えるためのライセンスを配信する送出装置と、前記ライセンスを取得し、前記ライセンスに基づきコンテンツをセキュアに利用する端末装置とから構成されるデジタル権利管理システムであって、前記送出装置は、前記ライセンスを生成するライセンス生成手段と、前記ライセンスに、ＩＤを付与するライセンスＩＤ付与手段と、前記ライセンスに、前記ライセンスの取得が可能な期限を示すライセンス取得期限を付与するライセンス取得期限付与手段と、前記ライセンスを前記端末装置に送出するライセンス送出手段とを備え、前記端末装置は、前記ライセンスを取得するライセンス取得手段と、少なくとも、前記ライセンスに付加された前記ライセンスＩＤと、前記ライセンス取得期限と、を含むライセンス取得履歴を記録するライセンス取得履歴記録手段と、前記ライセンスの取得時に、取得する前記ライセンスのライセンスＩＤと同一のライセンスＩＤが、前記ライセンス取得履歴記録手段が保持する前記ライセンス取得履歴に存在する場合には、前記ライセンスの取得を抑制するライセンス取得抑制手段とを備え、前記ライセンス取得履歴記録手段は、少なくとも前記ライセンス取得期限までは、前記ライセンスＩＤと前記ライセンス取得期限からなる前記ライセンス取得履歴を保持することを特徴とする。

【０００９】

本構成によって、ユーザによる不正なライセンス取得を防止するとともに、リストのサイズの増大を防止することが可能となる。

【発明の効果】

【００１０】

本発明によれば、端末装置で取得したライセンスのＩＤと有効期限とを、ライセンスの取得履歴として管理し、少なくともライセンスの取得期限までライセンス取得履歴を保持しておくことにより、無制限なライセンス取得の防止と、管理するデータサイズの増大の防止とを両立することが可能となる。

【発明を実施するための最良の形態】

【００１１】

以下、本発明における実施の形態について、図面を用いて詳細に説明する。

図１は、本発明における実施の形態に関わる、デジタル権利管理システムを用いたコンテンツ配信システム１の全体の概略構成を示す図である。

【００１２】

このコンテンツ配信システム１は、デジタル放送を通じて放送局に設置された送出装置から送出される暗号化コンテンツを、セキュアに利用制御を行いつつ、ユーザが端末装置において利用することが可能なシステムであって、コンテンツやコンテンツのライセンスなどを配信する放送局１０１と、コンテンツを利用する端末装置１０２と、端末装置１０２とともにコンテンツの利用に用いるＩＣカード１０３と、これらを相互に接続するデジタル放送１０４、および、通信ネットワーク１０５とから構成されている。

【００１３】

なお、端末装置１０２は複数あって良いが、図１では簡単のため、１つの端末装置１０２のみをその代表として示している。

放送局１０１は、暗号化されたコンテンツ（以下、暗号化コンテンツ）や、暗号化コンテンツを復号するための暗号鍵などを配信する送出装置などを有する。

【００１４】

端末装置１０２は、デジタル放送１０４や通信ネットワーク１０５などから暗号化コンテンツを受信するとともに、暗号化コンテンツを復号するためのライセンスを受信し、暗号化コンテンツを復号してコンテンツを利用するための装置である。また、端末装置１０２は、ＩＣカード１０３を挿入するインタフェースを有しており、高いセキュリティを必要とする処理については、ＩＣカード１０３と連携することにより処理を実行する。

【００１５】

ＩＣカード１０３は、耐タンパ化されたハードウェアモジュールである。具体的には、ＩＣカード１０３は、国内デジタル放送の標準ＣＡＳが実装されたＢ－ＣＡＳカードのような高度なセキュリティを有するカードや、ＳＤ（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ）カードにセキュリティプロセッサが搭載されたようなモジュールなどがあげられる。

【００１６】

デジタル放送１０４は、ＢＳ（Ｂｒｏａｄｃａｓｔｉｎｇ　Ｓａｔｅｌｌｉｔｅ）デジタル放送、ＣＳ（Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｓａｔｅｌｌｉｔｅ）デジタル放送、地上デジタル放送などの無線によるデジタル放送や、デジタルＣＡＴＶなどの有線によるデジタル放送である。

【００１７】

通信ネットワーク１０５は、放送局１０１と端末装置１０２とを相互に接続するネットワークである。例えば、通信ネットワーク１０５は、ＡＤＳＬ（Ａｓｙｍｍｅｔｒｉｃ　Ｄｉｇｉｔａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｌｉｎｅ）、ＦＴＴＨ（Ｆｉｂｅｒ　Ｔｏ　Ｔｈｅ　Ｈｏｍｅ）、双方向デジタルＣＡＴＶ、ＩＥＥＥ８０２．１１ｇなどの高速インターネット網である。

【００１８】

なお、放送局１０１および端末装置１０２の構成については、後で図を用いて詳細に説明する。

ここで、サーバ型放送方式における限定再生方式の暗号スキームについて、図２を用いて説明する。

【００１９】

図２において、コンテンツや暗号鍵を送出する送信側２００と、コンテンツや暗号鍵を受信する受信側２５０に分けて説明する。

送信側２００において、コンテンツは、スクランブル鍵Ｋｓ２０１と呼ばれる暗号鍵によってスクランブル、すなわち、暗号化（２０２）される。コンテンツのスクランブルについては、ＭＰＥＧ－２トランスポートストリーム（Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ、以下、ＴＳと記述）のパケット単位で、ＴＳパケットのペイロード部をスクランブルする。また、スクランブル鍵Ｋｓ２０１は、不正受信に対するセキュリティ向上のため、数秒おきに変更される時変鍵である。

【００２０】

また、コンテンツをスクランブルするスクランブル鍵Ｋｓ２０１は、悪意あるユーザなどによる不正な傍受を防止するため、ワーク鍵Ｋｗ２０３を用いて暗号化（２０４）される。ワーク鍵Ｋｗ２０３は、従来の一般的な限定受信方式で用いられている放送事業者毎の契約単位、グループ単位に割り当てられる暗号鍵であり、ワーク鍵Ｋｗ２０３自体のセキュリティを確保するため、数ヶ月～数年の期間で更新されるのが一般的である。少なくともスクランブル鍵Ｋｓ２０１を含み、コンテンツに関連する情報を送信するためのデータ構造は、ＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ）と呼ばれ、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓ（ＩＥＣ／ＩＳＯ１３８１８－１）のプライベートセクションとして構成される。ワーク鍵Ｋｗ２０３で暗号化されたＥＣＭは、ＥＣＭ－Ｋｗ

と呼ばれ、放送コンテンツのリアルタイム視聴において利用する。

【００２１】

また、スクランブル鍵Ｋｓ２０１は、コンテンツ鍵Ｋｃ２０５でも暗号化（２０４）される。コンテンツ鍵Ｋｃ２０５は、コンテンツ単位に割り当てられる暗号鍵であり、ＥＣＭ－Ｋｗと同様、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓのプライベートセクションとして構成される。少なくともスクランブル鍵Ｋｓ２０１を含むＥＣＭを、コンテンツ鍵Ｋｃ２０５で暗号化したものをＥＣＭ－Ｋｃと呼び、放送コンテンツの蓄積視聴（サーバ型放送方式におけるＴｙｐｅＩコンテンツ）において利用する。

【００２２】

さらに、コンテンツ鍵Ｋｃ２０５についても、悪意あるユーザなどによる不正な傍受を防止するため、ワーク鍵Ｋｗ２０３で暗号化（２０６）される。コンテンツ鍵Ｋｃ２０５を含み、ワーク鍵Ｋｗ２０３で暗号化されたＥＣＭをＫｃ伝送用ＥＣＭと呼び、放送コンテンツの蓄積視聴において利用する。Ｋｃ伝送用ＥＣＭは、ＥＣＭ－Ｋｗ、および、ＥＣＭ－Ｋｃと同様に、ＭＰＧＥ－２　Ｓｙｓｔｅｍｓのプライベートセクションとして構成されるものである。

【００２３】

ＥＣＭ－ＫｗやＫｃ伝送用ＥＣＭを暗号化するワーク鍵Ｋｗ２０３は、コンテンツの利用に先立って送信側２００と受信側２５０とで共有しておく必要があるため、ＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｍｅｓｓａｇｅ）と呼ばれるデータ構造を利用して両者で共有する。このとき、スクランブル鍵Ｋｓ２０１やコンテンツ鍵Ｋｃ２０５と同様、盗聴防止のため、マスタ鍵Ｋｍ２０７と呼ばれる端末装置１０２固有の暗号鍵で暗号化（２０８）する。このマスタ鍵Ｋｍ２０７についても、送信側２００と受信側２５０で予め共有しておく必要があるが、受信側２５０のマスタ鍵Ｋｍ２５２は、端末装置１０２のセキュアな部分や、セキュリティモジュールと呼ばれるハードウェア的に耐タンパ化されたモジュールなどに出荷時などに予め書き込まれることで設定される。

【００２４】

なお、ＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、Ｋｃ伝送用ＥＣＭ、ＥＭＭのデータ構造の例については、後で図を用いて詳細に説明する。

また、本暗号スキームにおいて、端末装置１０２では、マスタ鍵Ｋｍ２０７、ワーク鍵Ｋｍ２０３など、特にセキュリティを必要とする情報の管理および処理を、ＩＣカードで行うようにするようにしても良い。

【００２５】

また、本暗号スキームで使用する暗号アルゴリズムとしては、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などの共通鍵暗号方式が用いられる。

また、ワーク鍵Ｋｗ２０３については、送信側２００と受信側２５０との間でＳＡＣ（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ｃｈａｎｎｅｌ）を確立し、通信ネットワーク１０５を介してワーク鍵Ｋｗ２０３を共有するようにしても良い。

【００２６】

以上のように生成された暗号化コンテンツ、ＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、Ｋｃ伝送用ＥＣＭ、および、ＥＭＭは、ＭＰＥＧ－２　ＴＳパケット化され、必要に応じてＰＳＩ（Ｐｒｏｇｒａｍ　Ｓｐｅｃｉｆｉｃ　Ｉｎｆｏｒｍａｔｉｏｎ）／ＳＩ（Ｓｅｒｖｉｃｅ　Ｉｎｆｏｒｍａｔｉｏｎ）などのデータと多重化（２０９）された後、受信側２５０に送信される。

【００２７】

一方、受信側２５０では、送信側２００から送出されたＭＰＥＧ－２　ＴＳパケットを受信し、これらを分離（２５１）して、暗号化コンテンツ、ＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、Ｋｃ伝送用ＥＣＭ、および、ＥＭＭを取得する。

【００２８】

この暗号化されたＥＭＭは、受信側２５０で予め保持しているマスタ鍵Ｋｍ２５２を用いて復号（２５３）し、ワーク鍵Ｋｗ２０３を取得する。このワーク鍵Ｋｗ２０３は、受

信側２５０の不揮発性メモリなどで保持される。

【００２９】

コンテンツをリアルタイム視聴する場合、ＥＣＭ－Ｋｗを取得して、ワーク鍵Ｋｗ２０３により暗号化されたＥＣＭ－Ｋｗを復号（２５５）して、スクランブル鍵Ｋｓ２０１を取得する。スクランブル鍵Ｋｓ２０１によって暗号化コンテンツを復号（２５６）して、コンテンツを利用することが可能となる。

【００３０】

一方、コンテンツを蓄積視聴する場合、図示しない蓄積部に記録された暗号化コンテンツ、ＥＣＭ－Ｋｃ、Ｋｃ伝送用ＥＣＭを読み出す。Ｋｃ伝送用ＥＣＭについては、送信側２００からは繰り返し送出されるが、受信側２５０では１回だけ取得すれば良い。なお、ＥＣＭ－Ｋｗは、リアルタイム視聴時のみで使用されるため、受信側２５０では蓄積されない。

【００３１】

リアルタイム視聴の場合において説明した方法で取得したワーク鍵Ｋｗ２０３を用いて、暗号化されたＫｃ伝送用ＥＣＭを復号（２５４）して、コンテンツ鍵Ｋｃ２０５を取得する。これによりコンテンツ鍵Ｋｃ２０５によりＥＣＭ－Ｋｃを復号（２５５）し、暗号化コンテンツを復号（２５６）して、コンテンツを利用することが可能となる。

【００３２】

以上、図２を用いて、サーバ型放送方式の限定再生方式の暗号スキームについて説明した。以降、本発明における実施の形態では、図２で説明した暗号スキームに基づくデジタル権利管理システムについての説明を行う。

【００３３】

このようなコンテンツ配信システム１において、デジタル放送１０４を通じて、コンテンツ（番組）、ライセンスが配信され、端末装置１０２において、コンテンツ、ライセンスをＨＤＤなどに蓄積し、ライセンスに基づきコンテンツを利用する処理を、図３～図２２の図面を用いて詳細に説明する。

【００３４】

図３は、図１に示す放送局１０１の構成を示す機能ブロック図である。

放送局１０１は、契約情報を管理する契約情報管理ＤＢ３０１と、ワーク鍵を管理するワーク鍵ＤＢ３０２と、コンテンツに関連する属性情報を管理するコンテンツ属性情報ＤＢ３０３と、コンテンツ毎に割り当てられるコンテンツ鍵を管理するコンテンツ鍵ＤＢ３０４と、映像、音声などのコンテンツを管理するコンテンツＤＢ３０５と、端末装置１０２とのインタフェースを提供する通信部３０６と、ユーザの契約情報を管理する契約処理部３０７と、端末装置１０２毎の個別情報を生成するＥＭＭ生成部３０８と、ＥＭＭを暗号化するＥＭＭ暗号化部３０９と、全端末装置１０２に共通な情報を生成するＥＣＭ生成部３１０と、ＥＣＭを暗号化するＥＣＭ暗号化部３１１と、コンテンツをエンコードするコンテンツ符号化部３１２と、ＭＰＥＧ－２　ＴＳを多重化する多重化部３１３と、映像、音声などのＴＳパケットを暗号化するコンテンツ暗号化部３１４と、ＴＳ化されたコンテンツを送出するコンテンツ送出部３１５とで構成されている。

【００３５】

契約情報管理ＤＢ３０１は、ユーザのコンテンツの視聴契約に関する情報を管理するためのデータベースである。具体的には、契約情報管理ＤＢ３０１は、図４に示すように、ＩＣカード１０３毎の視聴契約に関連する情報や、マスタ鍵Ｋｍ２０７を一元管理する契約情報管理テーブル４００を有する。契約情報管理ＤＢ３０１は、主として、ＥＭＭ生成部３０８が、端末装置１０２毎に視聴契約情報を配信するためのＥＭＭを生成する際に参照する。

【００３６】

カードＩＤ４０１は、端末装置１０２に挿入するＩＣカード１０３を一意に識別し、契約処理を行ったＩＣカード１０３に対してＥＭＭ９００を送出するための宛て先となる情報である。

【００３７】
ティア契約ＩＤ４０２は、放送局１０１が提供するサービスに対する月極め契約（サブスクリプション）の識別をするためのＩＤであり、一種の契約形態を示している。例えば、スポーツに関するコンテンツを視聴できる「スポーツコンテンツパック」、映画コンテンツを視聴できる「映画コンテンツパック」などがあげられる。

【００３８】
ＰＰＶ契約ＩＤ４０３は、放送局１０１が提供するサービスに対するペイ・パー・ビューの視聴契約を識別するためのＩＤであり、ティア契約ＩＤ９０８と同様、一種の契約形態を示している。

【００３９】
有効期限４０４は、放送局１０１との契約期間を示すものであり、有効期限９０４までは、当該放送局１０１のコンテンツを利用することが可能となる。
蓄積暗号鍵Ｋｍ’４０５は、端末装置１０２において、コンテンツやライセンス（ＥＣＭなど）をＨＤＤなどに蓄積する場合に、コンテンツやライセンスを取得した端末装置１０２、すなわち、ＩＣカード１０３に、コンテンツやライセンスをバインドする際に用いる。

【００４０】
マスタ鍵Ｋｍ４０６は、ＩＣカード１０３固有の暗号鍵であり、ＥＭＭを暗号化する場合に用いる。ＩＣカード１０３では出荷時に埋め込まれる。
例えば、図４では、カードＩＤ４０１が「ＣＡＲＤ－ＩＤ－１」なるＩＣカード１０３は、ティア契約ＩＤ４０２が「ＴＩＥＲＣＯＮＴ－ＩＤ－１」、ＰＰＶ契約ＩＤ４０３が「ＰＰＶＣＯＮＴ－ＩＤ－１」であるサービスに加入しており、有効期限４０４が「２００４／４／１～２００５／３／３１」であり、蓄積暗号鍵Ｋｍ’４０５が「０ｘ１１１・・・１１１」、マスタ鍵Ｋｍ４０６が「０ｘ１１１・・・１１１」であることを示している。

【００４１】
ワーク鍵ＤＢ３０２は、ユーザが事業者と視聴契約を行った場合に送出するＥＣＭを暗号化する鍵を管理するためのデータベースであって、ワーク鍵管理テーブル５００を有する。ワーク鍵ＤＢ３０２は、ＥＣＭ－Ｋｗ、Ｋｃ伝送用ＥＣＭを暗号化する際に、ワーク鍵Ｋｗ２０３を提供したりする場合に用いられる。

【００４２】
具体的には、ワーク鍵ＤＢ３０２は、図５に示すように、ワーク鍵ＩＤ５０１、ワーク鍵Ｋｗ５０２、ワーク鍵利用開始日５０３の組を管理するワーク鍵管理テーブル５００を管理する。

【００４３】
例えば、図５では、ワーク鍵ＩＤ５０１「ＷＫ－ＩＤ－１」に対応するワーク鍵Ｋｗ５０２が「０ｘ１２３・・・ｃｄｆ」であり、ワーク鍵Ｋｗ５０２の利用開始日を示すワーク鍵利用開始日５０３が「２００３／１１／２４」であることを示している。また、ワーク鍵ＩＤ５０１は、暗号化されたＥＣＭにおいて、暗号化に用いたワーク鍵Ｋｗ２０３を特定するために用いられる情報であり、ＥＣＭ－Ｋｗのワーク鍵ＩＤ１１０４や、Ｋｃ伝送用ＥＣＭのワーク鍵ＩＤ１００４に設定される。

【００４４】
コンテンツ属性情報ＤＢ３０３は、コンテンツの利用条件や、当該コンテンツを視聴可能な契約の種類など、コンテンツ利用に関する種々の情報を管理するためのデータベースである。具体的には、コンテンツ属性情報ＤＢ３０３は、図６に示すように、コンテンツ配信システム１内でコンテンツを一意に特定するためのコンテンツＩＤ６０１と、コンテンツ配信システム１内でライセンスを一意に特定するためのライセンスＩＤ６０２と、利用条件６０３と、契約情報６０４と、ライセンス変換期限６０５とを有するコンテンツ属性情報管理テーブル６００を備えている。

【００４５】

例えば、コンテンツＩＤ６０１が「ＣＯＮＴＥＮＴ－ＩＤ－１」、ライセンスＩＤ６０２が「ＬＩＣＥＮＳＥ－ＩＤ－１」であるコンテンツは、利用条件６０３が「有効期限１ヶ月」、契約情報６０４が「ＴＩＥＲＣＯＮＴ－ＩＤ－１」、ライセンス変換期限６０５が「２００４／４／３０」であることから、放送局１０１と「ＴＩＥＲＣＯＮＴ－ＩＤ－１」なるサービスを契約し、「２００４／４／３０」までにライセンスを取得する処理を行った場合、コンテンツを蓄積してから１ヶ月間は当該コンテンツが再生可能であることを示している。なお、ライセンス変換期限６０５に関わるライセンス変換処理については、端末装置１０２の構成について説明する際に、詳細に説明する。

【００４６】

また、コンテンツＩＤ６０１が「ＣＯＮＴＥＮＴ－ＩＤ－２」なるコンテンツについては、契約情報６０４が「ＴＩＥＲＣＯＮＴ－ＩＤ－１、ＴＩＥＲＣＯＮＴ－ＩＤ－２」であることから、このコンテンツを視聴するためには、放送局１０１と「ＴＩＥＲＣＯＮＴＥＮＴ－ＩＤ－１」または「ＴＩＥＲＣＯＮＴ－ＩＤ－２」の少なくともどちらかのサービスを契約していることが必要となる。また、コンテンツＩＤ６０１が「ＣＯＮＴＥＮＴ－ＩＤ－４」なるコンテンツについては、契約情報６０４が「ＰＰＶＣＯＮＴ－ＩＤ－１」であることから、このコンテンツがＰＰＶコンテンツであることが示されている。

【００４７】

コンテンツ鍵ＤＢ３０４は、端末装置１０２に蓄積されたコンテンツを利用するためのライセンス毎（すなわち、コンテンツ毎）に割り当てられる暗号鍵を管理するデータベースである。

【００４８】

具体的には、コンテンツ鍵ＤＢ３０４は、コンテンツ配信システム１においてコンテンツをユニークに識別するための識別子であるコンテンツＩＤ７０１、コンテンツ配信システム１においてライセンスをユニークに識別するための識別子であるライセンスＩＤ７０２、ライセンスＩＤ７０２に設定するコンテンツ鍵Ｋｃ７０３から構成されるコンテンツ鍵管理テーブル７００を有する。

【００４９】

例えば、図７では、図７では、コンテンツ７０１が「ＣＯＮＴＥＮＴ－ＩＤ－１」に対応するライセンスＩＤ７０２が、「ＬＩＣＥＮＳＥ－ＩＤ－１」であり、これらに対応するコンテンツ鍵Ｋｃ７０３が、「０ｘ１２３・・・ｃｄｆ」であることを示している。

【００５０】

コンテンツＤＢ３０５は、コンテンツを蓄積するためのデータベースである。具体的には、コンテンツＤＢ３０５は、図８に示すように、コンテンツ配信システム１内でコンテンツを一意に特定するためのコンテンツＩＤ８０１と、コンテンツの名前を示すコンテンツ名称８０２と、コンテンツをデジタル放送で配信する日時を示す放送日時８０３と、コンテンツ毎のコンテンツＤＢ３０５におけるファイルの位置を示すファイル名８０４とを有するコンテンツ管理テーブル８００を備えている。

【００５１】

例えば、コンテンツＩＤ８０１が「ＣＯＮＴＥＮＴ－ＩＤ－１」のコンテンツは、コンテンツ名称８０２が「マンデースポーツ」であり、放送日時８０３が「２００４／４／８　２１：００：００」、コンテンツＤＢ３０５におけるファイル名８０４はＵＲＩ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｉｄｅｎｔｉｆｉｅｒ）が「／ＳＰＯＲＴ／・・・／ＭＯＮＳＰＯＲＴＳ．ＶＣ」（「・・・」はＵＲＩの一部が省略されていることを示している）であることを示している。

【００５２】

なお、コンテンツ管理テーブル８００は、アナログＶＣＲ（Ｖｉｄｅｏ　Ｃａｓｓｅｔｅ　Ｒｅｃｏｒｄｅｒ）であってもよいし、コンテンツ管理テーブル８００に代わり、ライブ放送（生放送）などを撮影するビデオカメラなどであっても良い。

【００５３】

通信部３０６は、通信ネットワーク１０５を通じて、端末装置１０２と通信するための

部である。
契約処理部３０７は、端末装置１０２からの視聴契約の申し込みを処理する部である。
【００５４】
具体的には、契約処理部３０７は、Ｗｅｂブラウザなどを通じて放送局１０１との視聴契約を受け付け、ユーザ（端末装置１０２）に対する視聴契約情報を、契約情報管理ＤＢ３０１に登録する。
【００５５】
ＥＭＭ生成部３０８は、ワーク鍵Ｋｗ２０３やユーザの契約情報などを含むＥＭＭを生成する部である。
具体的には、ＥＭＭ生成部３０８は、主として新規契約や契約変更が行われたユーザ（端末装置１０２、すなわち、ＩＣカード１０３）に対して、契約情報管理ＤＢ３０１から当該ユーザの契約内容であるティア契約ＩＤ４０２、ＰＰＶ契約ＩＤ４０３、有効期限４０４などを読み出し、ＥＭＭに設定する。
【００５６】
ここで、図９を用いて、ＥＭＭのデータ構造についての詳細な説明を行う。
図９は、主としてワーク鍵Ｋｗ２０１やユーザ毎（ＩＣカード１０３毎）の情報を伝送するＥＭＭのデータ構造の一例を示す図である。
【００５７】
図９に示したＥＭＭ９００は、カードＩＤ９０２、事業者ＩＤ９０３、有効期限９０４、ワーク鍵ＩＤ９０５、ワーク鍵Ｋｗ９０６、蓄積暗号鍵Ｋｍ’９０７、ティア契約ＩＤ９０８、ＰＰＶ契約ＩＤ９０９、改ざん検出９１０とから構成されている。また、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓのプライベートセクション形式でトランスポートストリームに多重化するため、セクションヘッダ９０１、セクションテーラ（誤り検出）９１１が付加されている。ＥＭＭ９００に示したデータの大部分は、ＩＣカード１０３に蓄積され、管理される。
【００５８】
カードＩＤ９０２は、コンテンツ配信システム１において、端末装置１０２に挿入するＩＣカード１０３を一意に識別し、契約処理を行ったＩＣカード１０３に対してＥＭＭ９００を送出するための宛て先となる情報である。
【００５９】
事業者ＩＤ９０３は、コンテンツ配信システム１において、サービスを提供する事業者を識別するコードであって、後述するワーク鍵ＩＤ９０５とともに参照される。
有効期限９０４は、放送局１０１との契約期間を示すものであり、有効期限９０４までは、当該放送局１０１のコンテンツを利用することが可能となる。
【００６０】
ワーク鍵ＩＤ９０５は、ＥＣＭを暗号化するワーク鍵Ｋｗ２０３を識別するための情報であり、ＩＣカード１０３で暗号化されたＥＣＭを復号する際には、ワーク鍵ＩＤ９０５と同様の情報がＥＣＭの非暗号化部分に設定されるので、ワーク鍵ＩＤ９０５を参照することにより、どのワーク鍵Ｋｗ２０３を用いて暗号化されたＥＣＭを復号すれば良いかを判別することができる。
【００６１】
ワーク鍵Ｋｗ９０６は、放送局１０１との契約に対してユーザに与えられる暗号化であり、ＩＣカード１０３で暗号化されたＥＣＭ－Ｋｗ、および、Ｋｃ伝送用ＥＣＭを復号する際に用いる。
【００６２】
蓄積暗号鍵Ｋｍ’９０７は、端末装置１０２において、コンテンツやライセンス（ＥＣＭなど）をＨＤＤなどに蓄積する場合に、コンテンツやライセンスを取得した端末装置１０２、すなわち、ＩＣカード１０３に、コンテンツやライセンスをバインドする際に用いる。
【００６３】

ティア契約ＩＤ９０８は、放送局１０１が提供するサービスに対する月極め契約（サブスクリプション）の識別をするためのＩＤであり、「標準パック」、「プレミアムパック」などの放送局１０１との契約形態を示している。

【００６４】

ＰＰＶ契約ＩＤ９０９は、放送局１０１が提供するサービスに対するペイ・パー・ビューの視聴契約を識別するためのＩＤであり、ティア契約ＩＤ９０８と同様、一種の契約形態を示している。

【００６５】

改ざん検出９１０は、暗号化したＥＭＭ９００の改ざんを検出するためのハッシュ値が設定される。ハッシュアルゴリズムは、ＡＥＳのＣＢＣモードで暗号化した結果であるＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）や、ＳＨＡ－２５６などを用いる。

【００６６】

なお、ここでは、ティア契約、ＰＰＶ契約については、ティア契約ＩＤ９０８、ＰＰＶ契約ＩＤ９０９をそのままＥＭＭ９００に設定する場合の例を説明したが、それぞれのＩＤをビットマップなどで表現したものをＥＭＭ９００で配信し、伝送すべき情報量とＩＣカード１０３での保持すべき情報量を削減するようにしても良い。

【００６７】

また、ここでは、ワーク鍵Ｋｗ２０３は事業者毎に割り当てる場合の例を説明したが、ティア契約ＩＤ毎などの契約毎にワーク鍵Ｋｗ２０３を割り当てるようにしても良い。

以上、図９を用いて、ＥＭＭ９００のデータ構造についての詳細な説明を行った。

【００６８】

ＥＭＭ暗号化部３０９は、ＡＥＳなどを用いて、ＥＭＭ生成部３０８で生成したＥＭＭ９００を暗号化する部である。

具体的には、ＥＭＭ暗号化部３０９は、ＥＭＭ生成部３０８で生成したＥＭＭ９００を、契約情報管理ＤＢ３０１から取得したマスタ鍵Ｋｍ２０７で暗号化し、多重化部３１３に送信する。ＥＭＭ９００を暗号化するにあたっては、暗号化モードは、ＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）＋ＯＦＢ（Ｏｕｔｐｕｔ　ＦｅｅｄＢａｃｋ）を用いる。

【００６９】

ＥＣＭ生成部３１０は、スクランブル鍵Ｋｓ２０１などを含むＥＣＭを生成する部である。具体的には、ＥＣＭ生成部３１０は、上流システムからの指示により、コンテンツの送出に合わせてＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、Ｋｃ伝送用ＥＣＭを生成する。ＥＣＭ－Ｋｗ、および、ＥＣＭ－Ｋｃの生成については、コンテンツのセキュリティを堅固なものとするため、数秒おきにスクランブル鍵Ｋｓを生成して、ＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃに設定する。Ｋｃ伝送用ＥＣＭの生成については、コンテンツ属性情報ＤＢ３０３、および、コンテンツ鍵ＤＢ３０４から、利用条件６０３やコンテンツ鍵Ｋｃ７０３などを取得して、Ｋｃ伝送用ＥＣＭに設定する。また、生成したスクランブル鍵Ｋｓ２０１を、コンテンツを暗号化するコンテンツ暗号化部３１４に送信する。

【００７０】

ここで、図１０～図１１を用いて、ＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、Ｋｃ伝送用ＥＣＭのデータ構造についての詳細な説明を行う。

図１０は、主としてスクランブル鍵Ｋｓ２０１を伝送するＥＣＭ－ＫｗおよびＥＣＭ－Ｋｃのデータ構造の一例を示す図である。

【００７１】

図１０に示したＥＣＭ－Ｋｗ１０００、および、ＥＣＭ－Ｋｃ１０２０は、スクランブル鍵Ｋｓ２０１やコンテンツに関する情報の伝送に用いられる情報であり、事業者ＩＤ１００２、ワーク鍵ＩＤ１００３、コンテンツＩＤ１００４、スクランブル鍵Ｋｓ１００５、契約判定情報１００６、改ざん検出１００７とから構成されている。また、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓのプライベートセクション形式でトランスポートストリームに多重化

するため、セクションヘッダ１００１、セクションテーラ（誤り検出）１００７が付加されている。

【００７２】

事業者ＩＤ１００２は、コンテンツ配信システム１において、サービスを提供する事業者を識別するコードであって、次に述べるワーク鍵ＩＤ１００３とともに参照される。

ワーク鍵ＩＤ１００３は、ＥＣＭを暗号化するワーク鍵Ｋｗ２０３を識別するための情報であり、ＥＣＭの非暗号化部分に設定される。ＩＣカード１０３で、暗号化されたＥＣＭを復号する場合には、ワーク鍵ＩＤ１００３を参照することにより、どのワーク鍵Ｋｗ２０３を用いてＥＣＭを復号すれば良いかを判別することができる。

【００７３】

コンテンツＩＤ１００４は、コンテンツ配信システム１内でコンテンツに対して一意に割り当てられる識別子であり、コンテンツの識別のために用いる。

スクランブル鍵Ｋｓ１００５は、コンテンツのＴＳパケットのペイロード部を暗号化する暗号鍵である。端末装置１０２が、数秒おきに変更されるスクランブル鍵Ｋｓ１００５を取得するために要する時間を短縮するため、一般的にはスクランブル鍵Ｋｓ１００５に複数の暗号鍵を設定する。

【００７４】

契約判定情報１００６は、当該コンテンツの属性を示す情報であり、端末装置１０２でコンテンツを視聴する場合に、当該コンテンツを視聴するための契約がなされているか否かを判定するために用いる。

【００７５】

改ざん検出１００７は、暗号化されるＥＣＭの改ざんを検出するためのハッシュ値が設定される。ハッシュアルゴリズムは、ＥＭＭ９００の場合と同様、ＡＥＳのＣＢＣ－ＭＡＣや、ＳＨＡ－２５６などを用いる。

【００７６】

次に、図１１は、主として蓄積視聴のためのＥＣＭ－Ｋｃ１０２０を復号するためのコンテンツ鍵Ｋｃ２０５を伝送するＫｃ伝送用ＥＣＭのデータ構造の一例を示す図である。

図１１に示したＫｃ伝送用ＥＣＭ１１００は、コンテンツ鍵Ｋｃ２０５やコンテンツの利用条件（ライセンス）の伝送に用いられる情報であり、事業者ＩＤ１１０２、サービスタイプ１１０３、ワーク鍵ＩＤ１１０４、契約判定情報１１０５、ライセンス変換期限１１０６、ライセンスＩＤ１１０７、ライセンス有効期限１１０８、コンテンツ鍵Ｋｃ１１０９、利用可能回数１１１０、書き出し可能回数１１１１、改ざん検出１１１２とから構成されている。また、ＥＣＭ－Ｋｃ１０００およびＥＣＭ－Ｋｃ１０２０と同様に、セクションヘッダ１１０１、セクションテーラ（誤り検出）１１１３が付加されている。

【００７７】

事業者ＩＤ１１０２、ワーク鍵ＩＤ１１０４、契約判定情報１１０５、改ざん検出１１１２については、ＥＣＭ－Ｋｃ１０００、および、ＥＣＭ－Ｋｃ１０２０における事業者ＩＤ１００２、ワーク鍵ＩＤ１００３、契約判定情報１００６、改ざん検出１００８の説明と同様であるので、ここでは説明を省略する。

【００７８】

サービスタイプ１１０３は、Ｋｃ伝送用ＥＣＭ１１００を含むコンテンツが、ティア契約で視聴可能なコンテンツであるのか、ＰＰＶ契約であって、別途購入処理を行うことによって視聴可能なコンテンツであるのか、を識別するためのフラグである。本発明の実施の形態においては、ティア契約を「ＴＩＥＲＣＯＮＴ」、ＰＰＶ契約を「ＰＰＶＣＯＮＴ」として、以下の説明を行う。

【００７９】

ライセンス変換期限１１０６は、ＩＣカード１０３において、Ｋｃ伝送用ＥＣＭ１１００を変換して、蓄積視聴用のライセンスを取得する処理の期限を示すものである。ライセンス変換とは、Ｋｃ伝送用ＥＣＭ１１００に含まれる情報を用いて、蓄積視聴用のライセンスをフォーマット変換により生成する処理を指す。このライセンス変換期限１１０６を

経過した場合には、Ｋｃ伝送用ＥＣＭ１１００から蓄積視聴に必要なライセンスを取得することはできず、ライセンス変換期限１１０６経過後に、別途、通信などを用いて取得する必要がある。

【００８０】

ライセンスＩＤ１１０７は、変換したライセンスをコンテンツ配信システム１内で一意に識別するためのコードであり、ＩＣカード１０３において、ライセンスの変換履歴としても用いる。

【００８１】

ライセンス有効期限１１０８は、当該ライセンスにより、コンテンツを視聴可能な期限を示すものである。

コンテンツ鍵Ｋｃ１１０９は、コンテンツ単位で割り当てられる１６バイト長の暗号鍵であり、ライセンスに含まれる暗号鍵である。

【００８２】

利用可能回数１１１０は、当該ライセンスにより、コンテンツを視聴可能な回数を示すものである。

書き出し可能回数１１１１は、当該ライセンスにより、コンテンツを蓄積媒体に書き出すことが可能な回数を示すものである。

【００８３】

なお、ワーク鍵Ｋｗ２０３で暗号化されたリアルタイム視聴用のＥＣＭ－Ｋｃ１０００と、コンテンツ鍵Ｋｓ２０５で暗号化された蓄積視聴用のＥＣＭ－Ｋｃ１０２０のフォーマットは同一であり、暗号化を行う暗号鍵（ワーク鍵Ｋｗ２０３とコンテンツ鍵Ｋｓ２０５）と、セクションヘッダ１００１に記載されるセクション識別情報（テーブルＩＤ、テーブルＩＤエクステンションなど）やＴＳパケットのＰＩＤ（Ｐａｃｋｅｔ　ＩＤ）などが異なる。

【００８４】

また、ライセンス変換期限１１０６を、ライセンス有効期限１１０８とは別に設けることによって、端末装置１０２にコンテンツおよびライセンスを大量に蓄積し、短期の視聴契約を行うことによって、視聴契約期間以外に蓄積した過去のライセンスも含めて、短期間に大量のライセンスを取得されてしまうという課題を解決することができる。この場合には、ライセンス変換期限１１０６は、比較的短い期限を設定すると良い。また、この目的のためには、必ずしもライセンス（Ｋｃ伝送用ＥＣＭ）毎にライセンス変換期限１１０６を設ける必要はなく、システム固定値としてＩＣカード１０３などがあらかじめ保持しておくようにしても良い。

【００８５】

以上、図１０～図１１を用いて、ＥＣＭ－Ｋｗ１０００、ＥＣＭ－Ｋｃ１０２０、Ｋｃ伝送用ＥＣＭ１１００のデータ構造についての詳細な説明を行った。

ＥＣＭ暗号化部３１１は、ＡＥＳなどを用いて、ＥＣＭ生成部３１０で生成したＥＣＭを暗号化する部である。具体的には、ＥＣＭ暗号化部３１１は、ＥＣＭ生成部３１０で生成したＥＣＭ－Ｋｗ１０００、および、Ｋｃ伝送用ＥＣＭ１１００を、ワーク鍵ＤＢ３０２から取得したワーク鍵Ｋｗ２０３で暗号化する。合わせて、ＥＣＭ生成部３１０で生成したＥＣＭ－Ｋｃ１０２０を、コンテンツ鍵ＤＢ３０４から取得したコンテンツ鍵Ｋｃ２０５で暗号化する。各ＥＣＭを暗号化するにあたっては、暗号化モードは、ＣＢＣ＋ＯＦＢを用いる。ＥＣＭ暗号化部３１１は、このように暗号化した各ＥＣＭを、多重化部３１３に送信する。

【００８６】

コンテンツ符号化部３１２は、端末装置１０２に送出するコンテンツをコンテンツＤＢ３０５から読み出し、コンテンツをＭＰＥＧ形式で符号化する部である。

具体的には、コンテンツ符号化部３１２は、ＭＰＥＧストリームを生成するリアルタイムエンコーダであって、上流システム（例えば、番組運行管理システムなど）の指示により、コンテンツＤＢ３０５から映像、音声などを読み出し、映像、音声、データなどのＭ

ＰＥＧ－２やＭＰＥＧ－４のＥＳ（Ｅｌｅｍｅｎｔａｒｙ　Ｓｔｒｅａｍ）を生成する。さらに、これらのＥＳを含むＰＥＳ（Ｐａｃｋｅｔｉｚｅｄ　Ｅｌｅｍｅｎｔａｒｙ　Ｓｔｒｅａｍ）パケットを生成し、最後にＭＰＥＧ－２　ＴＳパケット化して、多重化部３１３に送出する。

【００８７】

多重化部３１３は、コンテンツ符号化部３１２から受け取った映像、音声、データなどを含むトランスポートストリームと、ＥＣＭ暗号化部３１１から受け取ったＥＣＭのトランスポートストリームと、ＥＭＭ暗号化部３０９から受け取ったＥＭＭ９００のトランスポートストリームとを多重化し、多重化されたトランスポートストリームをコンテンツ暗号化部３１４に送出する部である。具体的には、多重化部３１３は、コンテンツ符号化部３１２から受信したＴＳパケット化されたコンテンツと、ＥＣＭ暗号化部３１１から受信したＴＳパケット化されたＥＣＭ－Ｋｗ１０００、ＥＣＭ－Ｋｃ１０２０、Ｋｃ伝送用ＥＣＭ１１００と、ＥＭＭ暗号化部３０９から受信したＴＳパケット化されたＥＭＭ９００とをＴＳ多重化して、端末装置１０２に送信するための多重化トランスポートストリームを生成する。

【００８８】

コンテンツ暗号化部３１４は、ＡＥＳなどを用いてコンテンツを暗号化することにより、コンテンツのスクランブルを行う部である。具体的には、コンテンツ暗号化部３１４は、ＴＳパケットのアダプテーションフィールドを除くペイロード部を、ＥＣＭ生成部３１０から取得したスクランブル鍵Ｋｓ２０１を用いて、ＣＢＣ＋ＯＦＢモードによって暗号化（スクランブル）する。

【００８９】

コンテンツ送出部３１５は、コンテンツ暗号化部３１４において暗号化されたＴＳパケットを、端末装置１０２に送出する部である。具体的には、コンテンツ送出部３１５は、コンテンツ暗号化部３１４から受け取ったトランスポートストリームを、放送波としてネットワーク１０３を通じて端末装置１０２に送出する。

【００９０】

なお、ここでは、コンテンツＤＢ３０５に蓄積されたコンテンツを読み出し、コンテンツ符号化部３１２においてリアルタイムエンコードする場合の例を示したが、あらかじめオフラインでＰＥＳ（ＥＳ）あるいはＴＳを生成しておき、コンテンツＤＢ３０５に蓄積しておくことにより、コンテンツ送出時にコンテンツ符号化部３１２におけるエンコード処理を省略するようにしても良い。

【００９１】

以上、図３～図１１を用いて、放送局１０１の構成についての詳細な説明を行った。

一方、図１２は、図１に示す端末装置１０２、および、ＩＣカード１０３の構成を示す機能ブロック図である。

【００９２】

まず、端末装置１０２を構成する機能ブロックについての説明を行う。

送受信部１２０１は、デジタル放送１０４、および、通信ネットワーク１０５を通じて、放送局１０１からのコンテンツやライセンスを受信したり、放送局１０１と通信したりするための部である。

【００９３】

分離部１２０２は、ＭＰＥＧ－２　ＴＳにより多重化された暗号化コンテンツを取得し、コンテンツとＥＣＭなどとを分離するための部である。

具体的には、分離部１２０２は、送受信部１２０１が受信したトランスポートストリームに含まれるＰＡＴ（Ｐｒｏｇｒａｍ　Ａｓｓｏｃｉａｔｉｏｎ　Ｔａｂｌｅ）、ＰＭＴ（Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）などのＰＳＩ情報を参照して、コンテンツの映像、音声、データや、ＥＣＭ－Ｋｗ１０００、ＥＣＭ－Ｋｃ１０２０、Ｋｃ伝送用ＥＣＭ１１００を含むＴＳパケットのＰＩＤを取得し、コンテンツとＥＣＭ－Ｋｃ１０２０などとを分離する。コンテンツ蓄積部１２０３にコンテンツを蓄積する場合には、ＰＡＴ、Ｐ

ＭＴなどのＰＳＩ情報から必要な情報を選択してＳＩＴ（Ｓｅｌｅｃｔｉｏｎ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔａｂｌｅ）、ＤＩＴ（Ｄｉｓｃｏｎｔｉｎｕｉｔｙ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔａｂｌｅ）などのＰＳＩ情報の生成を行い、受信したトランスポートストリームを、パーシャルトランスポートストリーム（以下、パーシャルＴＳと記述する）と呼ばれるストリームを生成する処理を行う。

【００９４】

蓄積部１２０３は、コンテンツやライセンスなどを蓄積するための部である。具体的には、蓄積部１２０３は、ＨＤＤなどの大容量不揮発性記憶媒体であり、分離部１２０２において受信したトランスポートストリームから生成した、映像、音声などのコンテンツやＥＣＭ－Ｋｃ１０２０などのライセンスを含むパーシャルＴＳを蓄積する。

【００９５】

蓄積管理部１２０４は、端末装置１０２の蓄積部１２０３に蓄積するコンテンツやライセンスを管理しており、蓄積したコンテンツやライセンスの一覧などをユーザに提示するための情報を有する。

【００９６】

コンテンツ復号部１２０５は、暗号化コンテンツを復号する部である。具体的には、コンテンツ復号部１２０５は、暗号化されたＭＰＥＧ－２　ＴＳのコンテンツを取得し、トランスポートストリームに含まれるＰＡＴ、ＰＭＴなどのＰＳＩ情報を参照して、コンテンツの映像、音声、データを含むＴＳパケットを取得する。そして、ＩＣカード１０３から取得するスクランブル鍵Ｋｓ２０１でＡＥＳ暗号化されたＴＳパケットのペイロード部分を復号する。

【００９７】

コンテンツ利用部１２０６は、ＩＣカード１０３から取得するスクランブル鍵Ｋｓ２０１とコンテンツの利用条件とを用いて、セキュアにコンテンツの利用を行うための部である。

【００９８】

具体的には、コンテンツ利用部１２０６は、リアルタイム視聴時においては、分離部１２０２から受け取ったトランスポートストリームからＥＣＭ－Ｋｗ１０００のＴＳパケットを取得し、ＥＣＭ－Ｋｗ１０００を再構成する。このようにして得られたＥＣＭ－Ｋｗ１０００をワーク鍵Ｋｗ２０３で復号して、コンテンツをデスクランブルするためのスクランブル鍵Ｋｓ２０１を取得し、コンテンツを復号する。一方、蓄積視聴時においては、蓄積部１２０３から読み出したトランスポートストリームから、Ｋｃ伝送用ＥＣＭ１１００をワーク鍵Ｋｗ２０３で復号して、ライセンスを取得する。そして、ライセンスに含まれる利用条件判定を行った上で、コンテンツを利用可能である場合のみ、ライセンスに含まれるコンテンツ鍵Ｋｃ２０５を用いて、ＥＣＭ－Ｋｃ１０２０を復号して、スクランブル鍵Ｋｓ２０１を取得する。さらに、コンテンツ利用部１２０６は、図１２に図示しないセキュアな計時部を用いて、コンテンツの利用時間などを計時することにより、利用条件に従ったコンテンツの利用を制御する。このような制御のもと、コンテンツ利用部１２０６は、ＭＰＧＥ－２あるいはＭＰＥＧ－４の映像、音声、データなどのＥＳをデコードして、図１２に示さないモニタなどに出力する。

【００９９】

なお、コンテンツの利用を終了した場合に、ＩＣカード１０３に対して、利用終了通知を通知するようにしても良い。

端末装置１０２における第１のカードＩ／Ｆ部１２０７は、端末装置１０２とＩＣカード１０３とのインタフェースを提供するための部である。

【０１００】

具体的には、第１のカードＩ／Ｆ部１２０７は、ＩＳＯ７８１６－４で規定されているＴ＝０プロトコルやＴ＝１プロトコルを処理し、端末装置１０２やＩＣカード１０３の他の機能ブロックとの間で相互にデータをやりとりするための手段を提供するものである。端末装置１０２とＩＣカード１０３との通信は、悪意あるユーザなどによる通信の傍受を

防止するため、少なくともセキュリティを要する情報の授受については、端末装置１０２とＩＣカード１０３との間で相互認証が行われ、ＳＡＣ（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ｃｈａｎｎｅｌ）を確立した上で行われる。

【０１０１】

ユーザＩ／Ｆ部１２０８は、端末装置１０２とユーザとのインタフェースを提供するための部である。

具体的には、ユーザＩ／Ｆ部１２０８は、ＢＭＬ（Ｂｒｏａｄｃａｓｔｉｎｇ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）ブラウザ、Ｗｅｂブラウザ、レジデントアプリケーションなどのＧＵＩ（Ｇｒａｐｈｉｃａｌ　Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）であり、図１２に示さないモニタなどを通じて、ユーザ要求を受け付けたり、ユーザにメッセージを提示したりする。

【０１０２】

以上、端末装置１０２を構成する機能ブロックについての説明を行った。

次に、ＩＣカード１０３を構成する機能ブロックについての説明を行う。

カード情報管理ＤＢ１２１０は、ユーザのコンテンツの視聴契約に関する情報を管理するためのデータベースである。具体的には、カード情報管理ＤＢ１２１０は、全事業者で共通の視聴契約に関連する情報を管理する共通情報テーブル１３００と、事業者毎の視聴契約に関する情報を管理する事業者別情報テーブル１４００とを有する。

【０１０３】

カード情報管理ＤＢ１２１０の共通情報テーブル１３００は、図１３に示すように、カードＩＤ１３０１と、マスタ鍵Ｋｍ１３０２と、蓄積暗号鍵Ｋｍ’１３０３とを管理する。

【０１０４】

カードＩＤ１３０１は、コンテンツ配信システム１内でＩＣカード１０３を一意に識別するためのＩＤであり、ＩＣカード１０３に予め書き込まれて出荷される。

マスタ鍵Ｋｍ１３０２は、ＥＭＭ９００を暗号化する場合に用いられるカードＩＤ１３０１固有の暗号鍵であり、カードＩＤ１３０１と同様、ＩＣカード１０３に予め書き込まれて出荷される。

【０１０５】

蓄積暗号鍵Ｋｍ’１３０３は、端末装置１０２の蓄積部１２０３でライセンスを蓄積する場合に、ライセンスの取得を行ったＩＣカード１０３にライセンスをバインドするための暗号鍵であり、ＥＭＭ９００の事業者ＩＤ９０３で指定されるＩＤである。

【０１０６】

一方、カード情報管理ＤＢ１２１０の事業者別情報テーブル１４００は、図１４に示すように、事業者ＩＤ１４０１と、ティア契約ＩＤ１４０２と、ＰＰＶ契約ＩＤ１４０３と、有効期限１４０４と、ワーク鍵ＩＤ１４０５と、ワーク鍵Ｋｗ１４０６とを管理する。

【０１０７】

事業者ＩＤ１４０１は、コンテンツ配信システム１内で一意に放送局１０１を識別するためのＩＤであり、ＥＭＭ９００の事業者ＩＤ９０３で指定されるＩＤである。

ティア契約ＩＤ１４０２は、ユーザが放送局１０１と月極めコンテンツの視聴契約を行ったサービスのＩＤであり、ＥＭＭ９００のティア契約ＩＤ９０８で指定されるＩＤである。

【０１０８】

ＰＰＶ契約ＩＤ１４０３は、ユーザが放送局１０１とＰＶＶコンテンツの契約を行ったサービスのＩＤであり、ＥＭＭ９００のＰＰＶ契約ＩＤ９０９で指定されるＩＤである。

有効期限１４０４は、放送局１０１との視聴契約における視聴期限を示すものであり、ＥＭＭ９００の有効期限９０４で指定される期限である。

【０１０９】

ワーク鍵ＩＤ１４０５は、コンテンツ配信システム１内で、放送局１０１から配布されるワーク鍵Ｋｗ２０３を一意に識別するためのＩＤであり、ＥＭＭ９００のワーク鍵ＩＤ

９０５で指定されるＩＤである。但し、ワーク鍵Ｋｗ２０３の識別については、事業者ＩＤ１４０１とワーク鍵ＩＤ１４０５との組により、コンテンツ配信システム１内でユニークとなることに注意されたい。

【０１１０】

ワーク鍵Ｋｗ１４０６は、放送局１０１から配布されるワーク鍵Ｋｗ２０３であり、ＥＭＭ９００のワーク鍵Ｋｗ９０６で指定される１６バイトのバイト列である。

例えば、図１４では、事業者ＩＤ１４０１が「ＳＥＲＶＩＣＥ－ＩＤ－１」である事業者との契約内容は、ティア契約ＩＤ１４０２が「ＴＩＥＲＣＯＮＴ－ＩＤ－１」、ＰＰＶ契約ＩＤ１４０３が「ＰＰＶＣＯＮＴ－ＩＤ－１」、有効期限１４０４が「２００４／４／１～２００５／３／３１」、ワーク鍵ＩＤ１４０５が「ＫＷ－ＩＤ－１」、ワーク鍵Ｋｗ１４０６が「０ｘ１１１・・・１１１」であることを示しており、「ＳＥＲＶＩＣＥ－ＩＤ－１」であるコンテンツは、ティアコンテンツ（Ｋｃ伝送用ＥＣＭ１１００のサービスタイプ１１０４が「ＴＩＥＲＣＯＮＴ」であるコンテンツ）とＰＰＶコンテンツ（Ｋｃ伝送用ＥＣＭ１１００のサービスタイプ１１０４が「ＰＰＶＣＯＮＴ」であるコンテンツ）の両方のコンテンツが視聴可能である。また、事業者ＩＤ１４０１が「ＳＥＲＶＩＣＥ－ＩＤ－１０」である事業者については、ティア契約ＩＤ１４０２が「－（未契約）」、ＰＰＶ契約ＩＤ１４０３が「ＰＰＶＣＯＮＴ－ＩＤ－１」であることから、「ＳＥＲＶＩＣＥ－ＩＤ－１」であるコンテンツは、ティアコンテンツについては視聴不可であるが、ＰＰＶコンテンツに関しては、別途購入処理を行うことによって視聴が可能である。

【０１１１】

なお、ここでは、ワーク鍵ＩＤ１４０５とワーク鍵１４０６の組は、最新の一組を保持する場合の例を示したが、ワーク鍵の運用を切り替える際のスムーズな移行を行うため、事業者別情報テーブル１４００においては、少なくとも二組のワーク鍵を保持できるようにしておくのが望ましい。

【０１１２】

変換履歴ＤＢ１２１１は、ライセンスの変換履歴を蓄積するためのデータベースである。具体的には、変換履歴ＤＢ１２１１は、Ｋｃ伝送用ＥＣＭ１１００に含まれる情報から、蓄積視聴用のライセンスが無制限に変換されることを防止するため、ライセンスの変換（以下、ライセンス変換と記述）が行われたことを示す変換履歴（Ｔｒａｎｓｆｏｒｍａｔｉｏｎ　Ｌｏｇ、以下、ＴＬと記述）を保持する。

【０１１３】

ここで、変換履歴ＤＢ１２１１に蓄積するＴＬのデータ構造の一例を、図１５を用いて説明する。

ＴＬ１５００は、ライセンス変換を行ったライセンスを識別するためのライセンスＩＤ１５０１と、ライセンス変換が可能な期間を示すライセンス変換期限１５０２との組から構成されており、これらの複数組をリストとして管理している。ＴＬ１５００の各レコードは、少なくとも、ライセンス変換期限１５０２を経過するまでは保持されるため、一度変換を行ったライセンスについては、さらなるライセンス変換を抑制することができ、その結果、１つのＫｃ伝送用ＥＣＭ１１００からは、１つのライセンスのみを取得することができるので、事業者の権利を確実に保護することができる。

【０１１４】

ライセンスＤＢ１２１２は、放送局１０１から取得したライセンスをセキュアに管理するためのデータベースである。具体的には、ライセンスＤＢ１２１２は、放送局１０１から取得したライセンスを蓄積、管理するとともに、端末装置１０２の蓄積部１２０３などのＩＣカード１０３の外部にライセンスを蓄積する場合において、ライセンスの改ざんなどの不正な行為を防止するため、ライセンスＤＢ１２１２中のライセンスのハッシュ値を管理する。

【０１１５】

第２のカードＩ／Ｆ部１２１３は、端末装置１０２における第１のカードＩ／Ｆ部１２０７と同様の機能ブロックであるため、ここでは説明を省略する。

ＥＣＭ／ＥＭＭ復号部１２１４は、端末装置１０２から受信した、暗号化されたＥＣＭ、および、暗号化されたＥＭＭ９００を復号するための部である。具体的には、ＥＣＭ／ＥＭＭ復号部１２１４は、第２のカードＩ／Ｆ部１２１３から暗号化ＥＣＭ－Ｋｗ１０００、暗号化ＥＣＭ－Ｋｃ１０２０、暗号化ＥＭＭ９００を受け取り、カード管理情報ＤＢ１２１０から、それぞれに対応するワーク鍵Ｋｗ２０３（１４０６）、マスタ鍵Ｋｍ２０７（１３０２）を読み出し、また、ライセンスＤＢ１２１２に保持されているライセンスからコンテンツ鍵Ｋｃ２０５を受け取り、暗号化ＥＣＭ－Ｋｗ１０００、暗号化ＥＣＭ－Ｋｃ１０２０、Ｋｃ伝送用ＥＣＭ１１００、暗号化ＥＭＭ９００の暗号を復号する。

【０１１６】

ＥＣＭ／ＥＭＭ処理部１２１５は、平文のＥＣＭやＥＭＭから必要な情報を抽出したり、処理したりするための部である。具体的には、ＥＣＭ／ＥＭＭ処理部１２１５は、ＥＣＭ／ＥＭＭ復号部１２１４から受け取ったＥＣＭ－Ｋｗ１０００、ＥＣＭ－Ｋｃ１０２０、Ｋｃ伝送用ＥＣＭ１１００、ＥＭＭ９００を解釈し、カード管理情報ＤＢ１２１０の構築に必要な情報を抽出して記録したり、端末装置１０２がコンテンツの再生に要するスクランブル鍵Ｋｓ２０１を、ＥＣＭ－Ｋｗ１０００やＥＣＭ－Ｋｃ１０２０から抽出して、端末装置１０２にレスポンスとして返送したりする。

【０１１７】

ライセンス変換処理部１２１６は、放送局１０１から受信したＥＣＭなどに含まれる情報（またはライセンスそのもの）を、蓄積コンテンツの利用を制御するためのライセンスに変換するとともに、変換したライセンスの数を管理するための部である。具体的には、ライセンス変換処理部１２１６は、放送局１０１から取得したＫｃ伝送用ＥＣＭ１１００に含まれる情報を、図１６に示す蓄積視聴用のライセンスのフォーマットに変換するとともに、変換したライセンスのライセンスＩＤと有効期限とを管理するための変換履歴であるＴＬ１５００を生成、管理する。

【０１１８】

ここで、ライセンス変換処理部１２１６が変換するライセンスの構成の一例を、図１６を用いて説明する。

ライセンス１６００は、コンテンツの利用を許諾する情報であり、ライセンス識別子１６０１と、ライセンスＩＤ１６０２と、有効期限１６０３と、再生回数１６０４と、書き出し回数１６０５と、コンテンツ鍵Ｋｃ１６０６と、ライセンス１６００の改ざんを検出するための改ざん検出１６０７とから構成されている。

【０１１９】

ライセンス識別子１６０１は、コンテンツ配信システム１で利用可能なライセンスを識別するための識別子である。例えば、「ＳＶ－ＤＲＭ　ＬＩＣＥＮＳＥ」のような識別子であり、ライセンス変換処理部１２１６であらかじめ保持している識別子である。

【０１２０】

ライセンスＩＤ１６０２は、コンテンツ配信システム１内でライセンスを一意に識別するための識別子である。ライセンスＩＤ１６０２は、Ｋｃ伝送用ＥＣＭ１１００のライセンスＩＤ１１０７の値を設定する。

【０１２１】

有効期限１６０３は、ライセンス１６００が利用可能な期間を示し、利用開始日時および利用終了日時を有する。有効期限１６０３は、Ｋｃ伝送用ＥＣＭ１１００のライセンス有効期限１１０８の値を設定する。

【０１２２】

再生回数１６０４は、コンテンツを再生可能な回数を示し、再生回数が０より大である場合には、再生が可能となる。再生回数１６０４は、Ｋｃ伝送用ＥＣＭ１１００の利用可能回数１１１０の値を設定する。

【０１２３】

書き出し回数１６０５は、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）やＢＤ（Ｂｌｕ－Ｒａｙ　Ｄｉｓｃ）などの記録媒体などへのコンテンツの複製回数を示

す。書き出し回数１６０５は、Ｋｃ伝送用ＥＣＭ１１００の書き出し可能回数１１１１の値を設定する。

【０１２４】

コンテンツ鍵Ｋｃ１６０６は、ＥＣＭ－Ｋｃ１０２０を復号するためのコンテンツ鍵Ｋｃ２０５を示す。コンテンツ鍵Ｋｃ２０５がバイナリ値で設定され、ＥＣＭ－Ｋｃ１０２０を復号する場合に用いる。コンテンツ鍵Ｋｃ１６０６は、Ｋｃ伝送用ＥＣＭ１１００のコンテンツ鍵Ｋｃ１１０９の値を設定する。

【０１２５】

改ざん検出１６０７は、ライセンス１６００をハードディスクなどの非セキュアな領域に蓄積する場合に、改ざんの検出を行い、その正当性を確保するためのものであって、ライセンス１６００の内容が更新される度に、ライセンス１６００の改ざんを防止したい箇所（典型的には、ライセンス識別子１６０１～コンテンツ鍵Ｋｃ１６０６）についてハッシュ値を計算し、計算結果を管理する。このハッシュ値は、ハード的に耐タンパ化されたＩＣカード１０３の内部で管理する。ハッシュアルゴリズムとしては、例えば、ＳＨＡ－１（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ　１）や、ＳＨＡ－２５６などが挙げられる。また、ライセンス１６００をハードディスクなどの非セキュアな領域に蓄積する場合には、少なくともコンテンツ鍵Ｋｃ１６０６の部分は暗号化されて蓄積される。

【０１２６】

以上、図１６を用いて、コンテンツ配信システム１におけるライセンス１６００の構成の説明を行った。

ライセンス処理部１２１７は、ライセンスに基づき、コンテンツの利用可否判定をセキュアに行う。

【０１２７】

具体的には、ライセンス処理部１２１７は、ユーザからライセンスの利用要求を受けた場合に、放送局１０１から取得したライセンスに含まれる利用条件に基づき、コンテンツの利用が可能かどうかを判定する。そして、利用条件がコンテンツの利用を許諾している場合に限り、ＥＣＭ－Ｋｃ１０２０を復号するためのコンテンツ鍵Ｋｃ２０５をＥＣＭ／ＥＭＭ復号部１２１４に渡す、という処理を行う。

【０１２８】

例えば、ライセンス処理部１２１７は、ライセンス１６００に設定された有効期限１６０３を参照し、コンテンツが利用可能であるかどうかを判定する。端末装置１０２に保持している、図１２には図示しないセキュアな計時部により提供される現在時刻を参照し、現在時刻が有効期限１６０３内である場合は、コンテンツの再生が可能である、というような判定処理を行う。

【０１２９】

以上、図１２～図１６を用いて、端末装置１０２およびＩＣカード１０３についての詳細な構成の説明を行った。

さて、以上のように構成された端末装置１０２およびＩＣカード１０３において、ユーザが放送局１０１との視聴契約を行い、放送局１０１の配信装置からコンテンツおよびライセンスを取得して、端末装置１０２に蓄積し、端末装置１０２においてコンテンツを利用するという一連の動作を、図１７～図２２に示すフローチャートを用いて説明する。

【０１３０】

なお、図１７～図２２に示すフローチャートにおいて、ユーザがＰＰＶコンテンツを利用する場合には、コンテンツの購入処理が必要であるが、これらの処理については本発明の主眼ではないため、以下では説明を省略する。

【０１３１】

最初に、端末装置１０２において、ユーザが放送局１０１と視聴契約を行う動作を、図１７に示すフローチャートを用いて説明する。

まず端末装置１０２において、ユーザが、ユーザＩ／Ｆ部１２０８が提供するＧＵＩにより、放送局１０１との視聴契約を行う（ステップＳ１７０１）。

【０１３２】
具体的には、ユーザが、ユーザＩ／Ｆ部１２０８が提供するＧＵＩによって、放送局１０１が提供するティア契約、または、ＰＰＶ契約の視聴契約のうち所望の契約を選択すると、ユーザＩ／Ｆ部１２０８は、対応する契約を識別するためのＩＤ（以下、契約ＩＤと記述）を、ＩＣカード１０３のカードＩＤ１３０１などとともに送受信部１２０１に送信する。送受信部１２０１は、放送局１０１とＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）などを用いてＳＡＣを確立し、受け取った契約ＩＤとカードＩＤ１３０１とを放送局１０１に送信する。なお、ユーザＩ／Ｆ部１２０８は、Ｗｅｂブラウザなどによってあらかじめ契約ＩＤを取得済みであるものとする。また、カードＩＤ１３０１についても、ＩＣカード１０３の挿入時などにあらかじめ取得済みであるものとする。

【０１３３】
放送局１０１は、端末装置１０２からの視聴契約の申し込みを受け付ける（ステップＳ１７０２）。
具体的には、放送局１０１の通信部３０６は、端末装置１０２から契約ＩＤなどを受信すると、契約ＩＤを契約処理部３０７に渡す。

【０１３４】
放送局１０１は、端末装置１０２から受信した契約ＩＤに基づき、契約処理を行い、ユーザの契約に関する情報をデータベースに登録する（ステップＳ１７０３）。
具体的には、契約処理部３０７は、必要に応じて、クレジットカード番号や銀行口座番号などを用いて課金処理を行い、契約情報管理ＤＢ３０１にユーザの視聴契約情報を登録する。このとき契約処理部３０７は、合わせて、ＩＣカード１０３固有の蓄積暗号鍵Ｋｍ’３０５を生成し、ＩＣカード１０３固有のマスタ鍵Ｋｍ３０６とともに、契約情報管理ＤＢ３０１に登録する。

【０１３５】
なお、ＩＣカード１０３毎に固有のマスタ鍵Ｋｍ３０６については、鍵管理センタなどからあらかじめ取得しておくものとする。
放送局１０１のＥＭＭ生成部３０８は、視聴契約を行ったユーザに対するＥＭＭ９００を生成する（ステップＳ１７０４）。

【０１３６】
具体的には、ＥＭＭ生成部３０８は、顧客管理システムなどの上位のシステムからの随時または一日一回などのＥＭＭ送出指示に基づき、契約情報管理ＤＢ３０１の契約情報管理テーブル４００から、ＥＭＭ９００を送出すべきカードＩＤ４０１のティア契約ＩＤ４０２～蓄積暗号鍵Ｋｍ’４０５を抽出し、該当カードＩＤ４０１宛てのＥＭＭ９００を生成する。ＥＭＭ生成部３０８は、生成したＥＭＭ９００をＥＭＭ暗号化部３０９に送信する。

【０１３７】
放送局１０１のＥＭＭ暗号化部３０９は、生成したＥＭＭ９００に対応するマスタ鍵で、ＥＭＭ９００を暗号化する（ステップＳ１７０５）。
具体的には、ＥＭＭ暗号化部３０９は、ＥＭＭ生成部３０８から受け取ったＥＭＭ９００のカードＩＤ９０２を参照して、契約情報管理ＤＢ３０１の契約情報管理テーブル４００から、カードＩＤ４０１が合致するＩＣカード１０３のマスタ鍵Ｋｍ４０６を読み出す。このマスタ鍵Ｋｍ４０６を用いて、ＥＭＭ９００の必要部分をＡＥＳで暗号化する。ＥＭＭ暗号化部３０９は、暗号化したＥＭＭ９００を多重化部３１３に送信する。

【０１３８】
放送局１０１は、暗号化したＥＭＭ９００を、コンテンツなどと多重化し、端末装置１０２に送出する（ステップＳ１７０６）。
具体的には、多重化部３１３は、ＥＭＭ暗号化部３０９から受け取ったＥＭＭ９００と、コンテンツ符号化部３１２などから受け取ったコンテンツなどとをＴＳパケット化した後、ＴＳ多重化する。その後、コンテンツ暗号化部３１４において、コンテンツの必要部分がスクランブルされ、コンテンツ送出部３１５が、放送波としてＥＭＭ９００を含むＴ

Ｓを端末装置１０２に送出する。

【０１３９】

端末装置１０２は、自己宛てのＥＭＭ９００を受信する（ステップＳ１７０７）。

具体的には、端末装置１０２の送受信部１２０１および分離部１２０２は、事前にＩＣカード１０３から取得したカードＩＤを用いて、受信したＥＭＭ９００をフィルタリングし、自己宛てのＥＭＭ９００を抽出する。

【０１４０】

端末装置１０２の第１のカードＩ／Ｆ部１２０７は、受信したＥＭＭ９００をＩＣカード１０３に送出する（ステップＳ１７０８）。

ＩＣカード１０３の第２のカードＩ／Ｆ部１２１３は、端末装置１０２の第１のカードＩ／Ｆ部１２０７からＥＭＭ９００を受信する（ステップＳ１７０９）。

【０１４１】

ＩＣカード１０３は、ＩＣカード１０３内で、ＥＭＭ９００に含まれる情報を管理する（ステップＳ１７１０）。

具体的には、第２のカードＩ／Ｆ部１２１３が受信したＥＭＭ９００を、ＥＣＭ／ＥＭＭ復号部１２１４に送信する。ＥＣＭ／ＥＭＭ復号部１２１４は、ＥＭＭ９００のカードＩＤ９０２が自身のＩＣカード１０３が保持するカードＩＤと一致することを確認した上で、カード管理情報ＤＢ１２１０の共通情報テーブル１３００からマスタ鍵Ｋｍ１３０２を読み出し、ＥＭＭ９００のカードＩＤ９０２を復号する。復号後、ＥＭＭ９００の改ざん検出９１０を用いて、暗号化ＥＭＭ９００が正しく復号できたことを確認する。改ざんが発見された場合は、当該ＥＭＭ９００の処理を中断する。ＥＣＭ／ＥＭＭ復号部１２１４は、復号したＥＭＭ９００をＥＣＭ／ＥＭＭ処理部１２１５に渡す。ＥＣＭ／ＥＭＭ処理部１２１５は、受け取ったＥＭＭ９００を解釈し、必要な情報をカード管理情報ＤＢ１２１０に蓄積し、図１３および図１４に示した、共通情報テーブル１３００および事業者別情報テーブル１４００を構築する。

【０１４２】

なお、ここでは、端末装置１０２が通信ネットワーク１０５を通じて、放送局１０１に対して視聴契約の申し込みを行う場合の例を示したが、電話やハガキなどのオフラインによる視聴契約の申し込みであっても良い。

【０１４３】

次に、放送局１０１における送出装置が、コンテンツを送出する動作を、図１８に示すフローチャートを用いて説明する。

まず、ＥＣＭ生成部３１０は、コンテンツ送出指示を受信すると、コンテンツ送出開始に先立ち、Ｋｃ伝送用ＥＣＭ１１００を生成する（ステップＳ１８０１）。

【０１４４】

具体的には、ＥＣＭ生成部３１０は、番組運行管理装置などの上流システムからのコンテンツ送出指示、すなわち、ＥＣＭ生成指示をトリガとして、コンテンツ単位の暗号鍵を有するＫｃ伝送用ＥＣＭ１１００を生成するため、コンテンツ属性情報ＤＢ３０３およびコンテンツ鍵ＤＢ３０４を参照して、ライセンスＩＤ６０２、利用条件６０３、コンテンツ鍵Ｋｃ７０３などを読み出す。読み出した情報から、図１１に示したＫｃ伝送用ＥＣＭ１１００を生成する。ＥＣＭ生成部３１０は、生成したＫｃ伝送用ＥＣＭ１１００を、ＥＣＭ暗号化部３１１に送信する。

【０１４５】

ＥＣＭ暗号化部３１１は、ワーク鍵Ｋｗ２０３でＫｃ伝送用ＥＣＭ１１００を暗号化する（ステップＳ１８０２）。

具体的には、ＥＣＭ暗号化部３１１は、ワーク鍵ＤＢ３０２のワーク鍵管理テーブル５００のワーク鍵利用開始日５０３を参照して、現在使用中のワーク鍵Ｋｗ２０３を特定する。特定したワーク鍵ＩＤ５０１とワーク鍵Ｋｗ５０２を読み出し、ＥＣＭ生成部３１０から受信したＫｃ伝送用ＥＣＭ１１００の必要部分をＡＥＳでＣＢＣ＋ＯＦＢモードによる暗号化を施す。合わせて、Ｋｃ伝送用ＥＣＭ１１００のワーク鍵ＩＤ１１０４に、ワー

ク鍵ＩＤ５０１を設定する。ＥＣＭ暗号化部３１１は、暗号化したＫｃ伝送用ＥＣＭ１１００を多重化部３１３に送信する。

【０１４６】

コンテンツ符号化部３１２は、コンテンツの読み出し、送出を開始し、コンテンツ送出中はコンテンツの送出が完了したか否かを監視する（ステップＳ１８０３）。

具体的には、コンテンツ符号化部３１２は、ステップＳ１８０１において、ＥＣＭ生成部３１０が上流システムから受信したコンテンツ送出指示と同じ指示を受けて、コンテンツＤＢ３０５のコンテンツ管理テーブル８００から該当コンテンツを読み出し、コンテンツをＭＰＥＧエンコードによりコンテンツのＴＳを生成する。生成したＴＳを多重化部３１３に送信するとともに、コンテンツＤＢ３０５からのコンテンツの読み出し、および、多重化部３１３へのコンテンツの送信が完了したか否かを監視する。

【０１４７】

ステップＳ１８０３において、ＮＯである場合、すなわち、コンテンツの送信が完了していない場合は、ステップＳ１８０４を実行する。

ステップＳ１８０３において、ＹＥＳである場合、すなわち、コンテンツの送信が完了した場合には、本コンテンツ送出処理を終了する。

【０１４８】

ＥＣＭ生成部３１０は、コンテンツの送出開始に伴い、コンテンツをスクランブルするためのスクランブル鍵Ｋｓ２０１を生成する（ステップＳ１８０４）。

具体的には、ＥＣＭ生成部３１０は、数秒おきに更新されるスクランブル鍵Ｋｓ２０１を順次生成して、生成したスクランブル鍵Ｋｓ２０１をコンテンツ暗号化部３１４に逐次送信する処理を行う。

【０１４９】

ＥＣＭ生成部３１０は、コンテンツ属性情報からＥＣＭを生成する（ステップＳ１８０５）。

具体的には、コンテンツの送出に合わせて、コンテンツ属性情報ＤＢ３０３のコンテンツ属性情報管理テーブル６００の契約情報６０４などを読み出し、ＥＣＭ－Ｋｗ１０００、ＥＣＭ－Ｋｃ１０２０を生成する。ＥＣＭ生成部３１０は、生成したＥＣＭ－Ｋｗ１０００、ＥＣＭ－Ｋｃ１０２０を、ＥＣＭ暗号化部３１１に送信する。

【０１５０】

ＥＣＭ暗号化部３１１は、ワーク鍵Ｋｗ２０３でＥＣＭ－Ｋｗを暗号化する（ステップＳ１８０６）。

具体的には、ＥＣＭ暗号化部３１１は、ワーク鍵Ｋｗ２０３によるＫｃ伝送用ＥＣＭ１１００の暗号化と同様の方法で、ワーク鍵ＤＢ３０２のワーク鍵管理テーブル５００のワーク鍵利用開始日５０３を参照して、現在使用中のワーク鍵Ｋｗ２０３を特定し、ワーク鍵Ｋｗ５０２でＥＣＭ－Ｋｗ１０００をＡＥＳで暗号化する。ＥＣＭ暗号化部３１１は、暗号化したＥＣＭ－Ｋｗ１０００を多重化部３１３に送信する。

【０１５１】

ＥＣＭ暗号化部３１１は、コンテンツ鍵Ｋｃ２０５でＥＣＭ－Ｋｃを暗号化する（ステップＳ１８０６）。

具体的には、ＥＣＭ暗号化部３１１は、コンテンツ鍵ＤＢ３０４のコンテンツ鍵管理テーブル７００を参照して、送出するコンテンツとコンテンツＩＤ７０１およびライセンス７０２が一致するレコードのコンテンツ鍵Ｋｃ７０３を読み出す。ここで、送出するコンテンツのコンテンツＩＤとライセンスＩＤは、上流システムからのコンテンツ送出指示の際に、上流システムなどから取得済みであるとする。読み出したコンテンツ鍵Ｋｃ７０３を用いて、ＥＣＭ生成部３１０から受信したＫｃ伝送用ＥＣＭ１１００の必要部分をＡＥＳでＣＢＣ＋ＯＦＢモードによる暗号化を施す。ＥＣＭ暗号化部３１１は、暗号化したＥＣＭ－Ｋｃ１０２０を多重化部３１３に送信する。

【０１５２】

コンテンツ暗号化部３１４は、コンテンツやＥＣＭが多重化されたＴＳをスクランブル

する（ステップＳ１８０８）。

具体的には、コンテンツ暗号化部３１４は、多重化部３１３においてコンテンツのＴＳやＥＣＭ－Ｋｗ１０００、ＥＣＭ－Ｋｃ１０２０、Ｋｃ伝送用ＥＣＭ１１００などのＴＳを多重化したＴＳのうち、映像、音声、データなどのコンテンツのＴＳパケットを選択して、ＡＥＳのＣＢＣ＋ＯＦＢモードでＴＳパケットのペイロード部分をスクランブルする。

【０１５３】

コンテンツ送出部３１５は、暗号化されたＴＳを送出する（ステップＳ１８０９）。

具体的には、コンテンツ送出部３１５は、コンテンツ暗号化部３１４においてスクランブルされたＴＳを、放送波として端末装置１０２に送出する。

【０１５４】

なお、ここでは、コンテンツの送出開始に合わせて、スクランブル鍵Ｋｓ２０１、すなわち、ＥＣＭ－Ｋｗ１０００、ＥＣＭ－Ｋｃ１０２０の送出を行う場合の例を示したが、端末装置１０２において、コンテンツの先頭から確実にデスクランブル可能となるように、コンテンツの送出開始に先立ってＥＣＭ－Ｋｗ１０００、ＥＣＭ－Ｋｃ１０２０を多重、送出することが望ましい。

【０１５５】

以上、図１８を用いて、放送局１０１によるコンテンツの送出処理についての詳細な説明を終了する。

次に、端末装置１０２が、デジタル放送１０４からコンテンツを受信し、蓄積部１２０３に蓄積する動作を、図１９～図２１に示すフローチャート等を用いて説明する。

【０１５６】

図１９は、端末装置１０２およびＩＣカード１０３におけるコンテンツ受信およびライセンス変換処理を示すフローチャートである。ただし、本処理において、ＩＣカード１０３におけるライセンス変換可否判定処理については、別途、図２１に示すフローチャートを用いて説明する。

【０１５７】

まず、端末装置１０２における蓄積管理部１２０４は、蓄積部１２０３に蓄積するコンテンツの蓄積状況を監視し、コンテンツ蓄積が終了しているか否かを確認する（ステップＳ１９０１）。

【０１５８】

具体的には、蓄積管理部１２０４は、ユーザから指定されたサーバ型放送ＴｙｐｅＩコンテンツをチューニングし、パーシャルＴＳとして蓄積部１２０３に順次蓄積する。蓄積処理の間、ＰＳＩ／ＳＩ（Ｐｒｏｇｒａｍ　Ｓｐｅｃｉｆｉｃ　Ｉｎｆｏｒｍａｔｉｏｎ／Ｓｅｒｖｉｃｅ　Ｉｎｆｏｒｍａｔｉｏｎ）などを参照しながら、当該コンテンツを蓄積完了したか否かを監視する。

【０１５９】

ステップＳ１９０１において、ＹＥＳである場合、すなわち、コンテンツの蓄積が未完了である場合には、ステップＳ１９０２を実行する。

ステップＳ１９０１において、ＮＯである場合、すなわち、コンテンツの蓄積が完了した場合には、本コンテンツ蓄積処理を終了する。

【０１６０】

分離部１２０２は、Ｋｃ伝送用ＥＣＭ１１００を取得したか否かを判断する（ステップＳ１９０２）。

具体的には、分離部１２０２は、受信したＴＳのＰＡＴ、ＰＭＴなどを参照し、Ｋｃ伝送用ＥＣＭのＰＩＤが付与されたＴＳパケットからＫｃ伝送用ＥＣＭ１１００を再構成するが、１つのコンテンツ蓄積において、少なくとも１回取得すれば良いＫｃ伝送用ＥＣＭ１１００を取得したか否かを監視する。

【０１６１】

ステップＳ１９０２において、ＹＥＳである場合、すなわち、Ｋｃ伝送用ＥＣＭ１１０

０を未取得である場合には、ステップＳ１９０３を実行する。
ステップＳ１９０２において、ＮＯである場合、すなわち、Ｋｃ伝送用ＥＣＭ１１００を取得済みである場合には、ステップＳ１９１２を実行する。

【０１６２】

分離部１２０２は、Ｋｃ伝送用ＥＣＭを分離し、ＩＣカード１０３に送信する（ステップＳ１９０３）。
具体的には、分離部１２０２は、ステップＳ１９０２の処理において再構成したＫｃ伝送用ＥＣＭ１１００を取得して、第１のカードＩ／Ｆ部１２０７を通じて、ＩＣカード１０３に送信する。

【０１６３】

ＩＣカード１０３は、受信したＫｃ伝送用ＥＣＭ１１００を変換しても良いか否かを判定する（ステップＳ１９０４）。
具体的には、ＩＣカード１０３の第２のカードＩ／Ｆ部１２１３は、端末装置１０２の第１のカードＩ／Ｆ部１２０７が送信した、暗号化されたＫｃ伝送用ＥＣＭ１１００を受信し、暗号復号処理の後、ライセンス変換処理部１２１６は、ＩＣカード１０３内部に蓄積した変換履歴ＤＢ１２１１を用いて、ライセンス変換処理を行ってもよいか否かの判定処理を実行する。なお、本ライセンス変換可否判定処理の詳細については、後で図２１を用いて説明するので、ここでは詳細な説明は行わない。

【０１６４】

ＩＣカード１０３のライセンス変換処理部１２１６は、ライセンス変換可否判定処理の結果、ライセンス変換が許可されているか否かを確認する（ステップＳ１９０５）。
ステップＳ１９０５において、ＹＥＳである場合、すなわち、ライセンス変換が許可されている場合には、ステップＳ１９０６を実行する。

【０１６５】

ステップＳ１９０５において、ＮＯである場合、すなわち、ライセンス変換が許可されていない場合には、ステップＳ１９１０を実行する。
ライセンス変換処理部１２１６は、Ｋｃ伝送用ＥＣＭ１１００をライセンス変換し、蓄積視聴用のライセンス１６００を生成する（ステップＳ１９０６）。

【０１６６】

具体的には、ライセンス変換処理部１２１６は、Ｋｃ伝送用ＥＣＭ１１００に含まれるライセンスＩＤ１１０７、ライセンス有効期限１１０８などを取得して、図１６に示すようなライセンス１６００を生成する。

【０１６７】

ライセンス変換処理部１２１６は、変換したライセンスがティアコンテンツであるか、ＰＰＶコンテンツであるかを判定する（ステップＳ１９０７）。
具体的には、ライセンス変換処理部１２１６は、Ｋｃ伝送用ＥＣＭ１１００のサービスタイプ１１０３を参照して、サービスタイプ１１０３が「ＴＥＩＲＣＯＮＴ」（ティアコンテンツ）であるか、「ＰＰＶＣＯＮＴ」（ＰＰＶコンテンツ）であるかを判断する。

【０１６８】

ステップＳ１９０７において、ＹＥＳである場合、すなわち、ティアコンテンツである場合には、ステップＳ１９０８を実行する。
ステップＳ１９０７において、ＮＯである場合、すなわち、ＰＰＶコンテンツである場合には、ライセンス変換履歴を記録する必要がないので、ステップＳ１９０８を実行せず、ステップＳ１９０９を実行する。ただし、ＰＰＶコンテンツのライセンス１６００は、購入処理を経て初めて利用可能になるライセンスであるので、例えば、ライセンス変換直後には、ライセンス１６００と合わせて、当該ライセンスが未購入であることを示すフラグを保持するようにし、購入処理後にフラグを削除することにより、当該ライセンスが購入済みであることを示す、といった処理が必要である。

【０１６９】

ライセンス変換処理部１２１６は、当該ライセンスの変換履歴を記録する（ステップＳ

１９０８）。
具体的には、ライセンス変換処理部１２１６は、変換履歴ＤＢ１２１１に蓄積されているＴＬ１５００のライセンスＩＤ１５０１とライセンス変換期限１５０２に、Ｋｃ伝送用ＥＣＭ１１００のライセンスＩＤ１１０７とライセンス変換期限１１０６を追加する。
【０１７０】
ライセンス処理部１２１７は、変換したライセンスをライセンスＤＢ１２１２に蓄積する（ステップＳ１９０９）。
第２のカードＩ／Ｆ部１２１３は、端末装置１０２に対して、Ｋｃ伝送用ＥＣＭ１１００によるライセンス変換要求に対するレスポンスを送信する（ステップＳ１９１０）。
【０１７１】
具体的には、第２のカードＩ／Ｆ部１２１３は、当該コンテンツのライセンス変換が許可されており、ライセンス変換が完了したか、あるいは、当該コンテンツのライセンス変換が許可されていない、または、ライセンス変換に失敗した、などのレスポンスメッセージを生成して、端末装置１０２に送信する。
【０１７２】
なお、ステップＳ１９０５において、ＮＯである場合のように、当該コンテンツのライセンス変換が許可されていない場合には、図２０に示すようなメッセージをユーザに提示する。
【０１７３】
図２０は、ユーザＩ／Ｆ部１２０８がユーザに提示するウォーニングメッセージの一例を示す図である。モニタ２００１に表示されているメッセージ２００２は、ユーザがＩＣカード１０３において、コンテンツ「マンデースポーツ」のライセンスＩＤに対応するライセンスを既にライセンス変換し、取得しているため、これ以上は取得できない旨を示している。
【０１７４】
第１のカードＩ／Ｆ部１２０７は、ＩＣカード１０３からのレスポンスを受信する（ステップＳ１９１１）。
具体的には、第１のカードＩ／Ｆ部１２０７は、ＩＣカード１０３の第２のカードＩ／Ｆ部１２１３から、Ｋｃ伝送用ＥＣＭ１１００の送信に対するライセンス変換結果のレスポンスを受信する。
【０１７５】
端末装置１０２の蓄積管理部１２０４は、コンテンツを蓄積部１２０３に蓄積する処理を行う（ステップＳ１９１２）。
具体的には、蓄積管理部１２０４は、コンテンツ、ＥＣＭ－Ｋｃ１０２０、Ｋｃ伝送用ＥＣＭ１１００などのＴＳパケットを、順次蓄積部１２０３に蓄積するとともに、合わせて、ＰＭＴなどから生成したＳＩＴ、ＤＩＴも蓄積する。なお、何らかの原因によりＩＣカード１０３でのライセンス変換処理に失敗した場合でも、後で再度ライセンス変換を試みることができるように、コンテンツやＥＣＭ－Ｋｃ１０２０、Ｋｃ伝送用ＥＣＭ１１００の蓄積処理は継続する。
【０１７６】
以上、図１９を用いて、端末装置１０２におけるコンテンツ蓄積処理についての説明を行った。
次に、ＩＣカード１０３でのライセンス変換可否判定処理について、図２１を用いて詳細に説明する。
【０１７７】
まず、ＩＣカードのＥＣＭ／ＥＭＭ復号部１２１４は、カード管理情報ＤＢ１２１０を参照して、Ｋｃ伝送用ＥＣＭ１１００を復号するためのワーク鍵Ｋｗ２０３が存在するか否かを判定する（ステップＳ２１０１）。
【０１７８】
具体的には、ＥＣＭ／ＥＭＭ復号部１２１４は、カード管理情報ＤＢ１２１０の事業者

別情報テーブル１４００を参照して、Ｋｃ伝送用ＥＣＭ１１００の事業者ＩＤ１１０２と、事業者ＩＤ１４０１が一致する事業者ＩＤのレコードを検索して、ワーク鍵Ｋｗ１４０６を読み出す。このとき、端末装置１０２からＫｃ伝送用ＥＣＭ１１００と一緒に取得した現在時刻が、有効期限１４０４を超過していたり、Ｋｃ伝送用ＥＣＭ１１００のワーク鍵ＩＤ１１０４と事業者別情報テーブル１４００のワーク鍵ＩＤ１４０５が一致しない場合などには、ワーク鍵Ｋｗ２０３が存在しないものとして処理する。

【０１７９】

ステップＳ２１０１において、ＹＥＳである場合、すなわち、ワーク鍵Ｋｗ１４０６が存在する場合には、ステップＳ２１０２を実行する。

ステップＳ２１０１において、ＮＯである場合、すなわち、ワーク鍵Ｋｗ１４０６が存在しない場合には、ステップＳ２１１１を実行する。

【０１８０】

ＥＣＭ／ＥＭＭ復号部１２１４は、ワーク鍵Ｋｗ１４０６でＫｃ伝送用ＥＣＭ１１００を復号する（ステップＳ２１０２）。

具体的には、ＥＣＭ／ＥＭＭ復号部１２１４は、ステップＳ２１０１で取得したワーク鍵Ｋｗ１４０６で、ＡＥＳによりＫｃ伝送用ＥＣＭ１１００の暗号化部を復号し、Ｋｃ伝送用ＥＣＭ１１００の改ざん検出１１１０により、Ｋｃ伝送用ＥＣＭ１１００が改ざんされていないかを確認する。万一、Ｋｃ伝送用ＥＣＭ１１００が改ざんされていることが検出された場合には、ライセンス変換は許可できないので、ステップＳ２１１１を実行して、本処理を終了する（図２１には図示せず）。

【０１８１】

ＥＣＭ／ＥＭＭ処理部１２１５は、ＩＣカード１０３が、当該コンテンツを視聴するための契約を有しているか否かを判定する（ステップＳ２１０３）。

具体的には、ＥＣＭ／ＥＭＭ処理部１２１５は、Ｋｃ伝送用ＥＣＭ１１００の契約判定情報１１０５と、カード管理情報ＤＢ１２１０の事業者別情報テーブル１４００のティア契約ＩＤ１４０２またはＰＰＶ契約ＩＤ１４０３を比較して、いずれかのＩＤが一致するか否かの判定処理を行う。

【０１８２】

ステップＳ２１０３において、ＹＥＳである場合、すなわち、いずれかのＩＤが一致する場合には、ステップＳ２１０４を実行する。

ステップＳ２１０３において、ＮＯである場合、すなわち、いずれのＩＤも一致しない場合には、ステップＳ２１１１を実行する。

【０１８３】

ライセンス変換処理部１２１６は、Ｋｃ伝送用ＥＣＭ１１００がライセンス変換の期限内であるかどうかを判定する（ステップＳ２１０４）

具体的には、ライセンス変換処理部１２１６は、Ｋｃ伝送用ＥＣＭ１１００のライセンス変換期限１１０６を参照して、端末装置１０２からＫｃ伝送用ＥＣＭ１１００といっしょに取得した現在時刻と比較することにより、当該Ｋｃ伝送用ＥＣＭ１１００がライセンス変換期限内であるか否かを判定する。

【０１８４】

ステップＳ２１０４において、ＹＥＳである場合、すなわち、ライセンス変換期限１１０６が現在時刻よりも新である場合には、ライセンス変換期限内であると判定し、ステップＳ２１０５を実行する。

【０１８５】

ステップＳ２１０４において、ＮＯである場合、すなわち、ライセンス変換期限１１０６が現在時刻よりも旧である場合には、ライセンス変換期限外であると判定し、ステップＳ２１１１を実行する。

【０１８６】

ライセンス変換処理部１２１６は、変換履歴ＤＢ１２１１を参照して、該当ライセンスＩＤの変換履歴を検索する（ステップＳ２１０５）。

具体的には、ライセンス変換処理部１２１６は、変換履歴ＤＢ１２１１のＴＬ１５００を参照し、Ｋｃ伝送用ＥＣＭ１１００のライセンスＩＤ１１０７と一致するライセンスＩＤ１５０１のレコードを検索する。

【０１８７】

ライセンス変換処理部１２１６は、該当ライセンスＩＤの変換履歴が存在するか否かを判定する（ステップＳ２１０６）。

具体的には、ライセンス変換処理部１２１６は、ステップＳ２１０５の検索結果を参照し、Ｋｃ伝送用ＥＣＭ１１００のライセンスＩＤ１１０７とＴＬ１５００のライセンスＩＤ１５０１が一致するレコードが存在するか否かを確認する。

【０１８８】

ステップＳ２１０６において、ＹＥＳである場合、すなわち、該当ライセンスＩＤの変換履歴が存在しない場合には、ステップＳ２１０７を実行する。

ステップＳ２１０６において、ＮＯである場合、すなわち、該当ライセンスＩＤの変換履歴が存在する場合には、ステップＳ２１１１を実行する。

【０１８９】

ライセンス変換処理部１２１６は、ＴＬ１５００に空きレコードまたは有効期限を超過したレコードが存在するか否かを検索する（ステップＳ２１０７）。

具体的には、ライセンス変換処理部１２１６は、新たにライセンス変換を行うライセンスＩＤを追記するレコードを発見するため、ＴＬ１５００を参照して、空きレコードを検索する。空きレコードが存在しない場合は、ＴＬ１５００のライセンス変換期限１５０２と、端末装置１０２からＫｃ伝送用ＥＣＭ１１００と一緒に取得した現在時刻を比較し、ライセンス変換期限１５０２が現在時刻より新であるレコードを検索する。

【０１９０】

ライセンス変換処理部１２１６は、変換履歴ＤＢ１２１１に空きレコードもしくはライセンス変換期限を超過しているレコードが存在するか否かを判定する（ステップＳ２１０８）。

【０１９１】

具体的には、ライセンス変換処理部１２１６は、ステップＳ２１０７の検索結果を参照し、ＴＬ１５００に空きレコードをもしくはライセンス変換期限１５０２を超過しているレコードが存在するか否かを判定する。

【０１９２】

ステップＳ２１０８において、ＹＥＳである場合、すなわち、空きレコードまたはライセンス変換期限１５０２を超過しているレコードが存在する場合には、ステップＳ２１０９を実行する。

【０１９３】

ステップＳ２１０８において、ＮＯである場合、すなわち、空きレコードまたはライセンス変換期限１５０２を超過しているレコードが存在しない場合には、これ以上ライセンス変換を実行することはできないため、ステップＳ２１１１を実行する。

【０１９４】

ライセンス変換処理部１２１６は、ステップＳ２１０８で判定した結果に基づき、空きレコードがない場合には、ライセンス変換期限１５０２を超過したレコードを削除し、新たなライセンスＩＤ１５０１の追加をできるようにする（ステップＳ２１０９）。

【０１９５】

ライセンス変換処理部１２１６は、当該Ｋｃ伝送用ＥＣＭ１１００のライセンスを変換を許可と判定し、本ライセンス変換可否判定処理を終了する（ステップＳ２１１０）。

ライセンス変換処理部１２１６は、当該Ｋｃ伝送用ＥＣＭ１１００のライセンスを変換は不許可と判定し、本ライセンス変換可否判定処理を終了する（ステップＳ２１１１）。

【０１９６】

以上、図１９～図２１を用いて、コンテンツ蓄積時の端末装置１０２およびＩＣカード１０３の処理の詳細について説明を行った。

最後に、端末装置１０２が、蓄積部１２０３のコンテンツを蓄積視聴する動作を、図２２に示すフローチャートを用いて説明する。

【０１９７】

まず、ユーザが視聴したい蓄積コンテンツのライセンスＩＤを指定すると、端末装置１０２は、ＩＣカード１０３に対してコンテンツ鍵を要求する（ステップＳ２２０１）。

具体的には、端末装置１０２のユーザＩ／Ｆ部１２０８は、メタデータなどを利用して、ユーザが再生したいコンテンツのライセンスＩＤを取得し、ライセンスＩＤをＩＣカード１０３に送信するため、第１のカードＩ／Ｆ部１２０７に送信する。第１のカードＩ／Ｆ部１２０７は、受信したライセンスＩＤをＩＣカード１０３に送信する。

【０１９８】

ＩＣカード１０３は、ライセンスＤＢ１２１２から該当ライセンスＩＤを有するライセンスを検索する（ステップＳ２２０２）

具体的には、ＩＣカード１０３の第２のカードＩ／Ｆ部１２１３は、受信したライセンスＩＤをライセンス処理部１２１７に送信し、ライセンス処理部１２１７はライセンスＩＤをキーとして、ライセンスＤＢ１２１２を検索する。

【０１９９】

ライセンス処理部１２１７は、要求されたライセンスＩＤと一致する、有効なライセンスが存在するか否かを判定する（ステップＳ２２０３）。

ステップＳ２２０３において、ＹＥＳである場合、すなわち、有効なライセンスが存在する場合には、ステップＳ２２０４を実行する。

【０２００】

ステップＳ２２０３において、ＮＯである場合、すなわち、有効なライセンスが存在しない場合には、再生不可として、ステップＳ２２０５を実行する。

ライセンス処理部１２１７は、取得したライセンスからコンテンツ鍵と利用条件を取得する（ステップＳ２２０４）。

【０２０１】

具体的には、ライセンス処理部１２１７は、取得したライセンス１６００から、コンテンツ鍵Ｋｃ１６０６と、有効期限１６０３、再生回数１６０４、書き出し回数１６０５を取得する。まず、有効期限１６０３～書き出し回数１６０５のコンテンツの利用条件については、ライセンス処理部１２１７において、有効期限１６０３と現在時刻との比較により、ライセンスが有効であるか否かを判定する。同様に、再生回数１６０４および書き出し回数１６０５については、ここではユーザがコンテンツの再生を要求していることから、再生回数１６０４を参照し、再生回数１６０４が０より大であるか否かを判定する。この利用条件判定において、コンテンツ利用可と判定された場合には、ライセンス処理部１２１７は、コンテンツ再生と同期して端末装置１０２から受け取る暗号化ＥＣＭ－Ｋｃ１０２０を復号するため、コンテンツ鍵Ｋｃ１６０６をＥＣＭ／ＥＭＭ復号部１２１４に送信する。コンテンツ鍵Ｋｃ１６０６は、当該コンテンツの再生の間は、ＥＣＭ／ＥＭＭ復号部１２１４において保持される。

【０２０２】

第２のカードＩ／Ｆ部１２１３は、端末装置１０２に対して、ライセンス処理結果のレスポンスを送信する（ステップＳ２２０５）。

具体的には、第２のカードＩ／Ｆ部１２１３は、ライセンス処理部１２１７による当該ライセンスの検索、および、ライセンスの利用可否判定の結果を取得して、端末装置１０２の第１のカードＩ／Ｆ部１２０７に対して、レスポンスとしてその旨を送信する。

【０２０３】

端末装置１０２の第１のカードＩ／Ｆ部１２０７は、ＩＣカード１０３からのレスポンスを受信して、コンテンツ復号部１２０５に送信し、コンテンツ復号部１２０５は当該コンテンツが再生可能かどうかを確認する（ステップＳ２２０６）。

【０２０４】

ステップＳ２２０６において、ＹＥＳである場合、すなわち、コンテンツが再生可能で

ある場合には、ステップＳ２２０７を実行する。
ステップＳ２２０６において、ＮＯである場合、すなわち、コンテンツが再生不可である場合には、本コンテンツ利用処理を終了する。
【０２０５】
蓄積管理部１２０４は、蓄積部１２０３から該当コンテンツを読み出し、コンテンツ復号部１２０５およびコンテンツ利用部１２０６が暗号化コンテンツの復号、および、コンテンツのデコードを開始する（ステップＳ２２０７）。
【０２０６】
蓄積管理部１２０４は、蓄積部１２０３から該当コンテンツの全ＴＳパケットを読み出し、コンテンツの再生が終了したか否かを判定する（ステップＳ２２０８）。
ステップＳ２２０８において、ＮＯである場合、すなわち、コンテンツの再生が継続中である場合には、ステップＳ２２０９を実行する。
【０２０７】
ステップＳ２２０８において、ＹＥＳである場合、すなわち、コンテンツの再生が終了した場合には、本コンテンツ再生処理を終了する。
分離部１２０２は、蓄積管理部１２０４が読み出した該当コンテンツからＥＣＭ－Ｋｃ１０２０を受け取り、ＩＣカード１０３に送信する（ステップＳ２２０９）。
【０２０８】
具体的には、分離部１２０２は、該当コンテンツからＥＣＭ－Ｋｃ１０２０のＰＩＤのＴＳパケットを取得し、ＥＣＭ－Ｋｃ１０２０を再構成する。再構成したＥＣＭ－Ｋｃ１０２０を、第１のカードＩ／Ｆ部に渡し、第１のカードＩ／Ｆ部１２０７がＩＣカード１０３にＥＣＭ－Ｋｃ１０２０を送信する。なお、ＥＣＭ－Ｋｃ１０２０に含まれるスクランブル鍵Ｋｓ２０１は数秒おきに更新されるため、本ステップの処理は数秒に１回の割合で行う必要がある。
【０２０９】
ＩＣカード１０３は、コンテンツ鍵Ｋｃ２０５によって受信したＥＣＭ－Ｋｃ１０２０を復号する（ステップＳ２２１１）。
具体的には、ＩＣカード１０３の第２のカードＩ／Ｆ部１２１３が端末装置１０２の第１のカードＩ／Ｆ部１２０７から受信したＥＣＭ－Ｋｃ１０２０を、ＥＣＭ／ＥＭＭ復号部１２１４に送信し、ＥＣＭ／ＥＭＭ復号部１２１４は、保持しているコンテンツ鍵Ｋｃ１６０６でＥＣＭ－Ｋｃ１０２０を復号する。
【０２１０】
ＩＣカード１０３は、ＥＣＭ－Ｋｃ１０２０から取得したスクランブル鍵Ｋｃ２０１を端末装置１０２に送信する（ステップＳ２２１２）。
具体的には、ＩＣカード１０３のＥＣＭ／ＥＭＭ処理部１２１５は、復号したＥＣＭ－Ｋｃ１０２０からスクランブル鍵Ｋｓ２０１を取得し、第２のカードＩ／Ｆ部１２１３を通じて、端末装置１０２にスクランブル鍵Ｋｓ２０１を送信する。なお、この際に、ライセンス１６００に設定されたコンテンツの利用条件を参照して、スクランブル鍵Ｋｃ２０１を端末装置１０２に送信するか否かを判定するようにしても良い。
【０２１１】
端末装置１０２のコンテンツ復号部１２０５は、ＩＣカード１０３から取得したスクランブル鍵Ｋｓ２０１で、コンテンツをデスクランブルし、コンテンツ利用部１２０６がコンテンツをデコードする（ステップＳ２２１０）。
【０２１２】
具体的には、コンテンツ復号部１２０５は、第１のカードＩ／Ｆ部１２０７から、ＩＣカード１０３より取得したスクランブル鍵Ｋｓ２０１を逐次受け取り、コンテンツ復号部１２０５に設定する。蓄積部１０３から読み出したコンテンツの暗号化ＴＳパケットを、スクランブル鍵Ｋｓ２０１を用いてデスクランブルし、コンテンツ利用部１２０６に送信する。コンテンツ利用部１２０６は、コンテンツ復号部１２０５から受信したデスクランブル後のコンテンツをＭＰＥＧデコードし、図示しないモニタなどに出力する。

【０２１３】
なお、端末装置１０２のコンテンツ復号部１２０５やコンテンツ利用部１２０６、あるいは、ＩＣカード１０３のＥＣＭ／ＥＭＭ復号部１２１４などにおいて利用条件に基づき、有効期間、累積の利用時間などのコンテンツの利用制御を行うようにしても良い。この場合、ライセンス１６００には、対応した利用条件が含まれるものとする。
【０２１４】
以上、図２２を用いて、端末装置１０２およびＩＣカード１０３におけるコンテンツ利用処理について説明した。
以上のように、コンテンツ配信システム１に適用したデジタル権利管理システムでは、端末装置で取得したライセンスのＩＤと有効期限とを、ライセンスの取得履歴として管理し、少なくともライセンスの取得期限までライセンス取得履歴を保持しておくようにしている。そのため、無制限なライセンス取得の防止と、管理するデータサイズの増大の防止とを両立することでき、事業者の権利を十分保護することが可能となる。
【０２１５】
なお、本発明における実施の形態では、サーバ型放送方式のＫｃ伝送用ＥＣＭ１１００を用いて、放送局１０１の送出装置から端末装置１０２およびＩＣカード１０３に対して、ライセンス１６００に設定する情報を配信するようにしたが、これに限られるものではなく、サーバ型放送方式のＥＣＭ－Ｋｗ１０００、ＥＣＭ－Ｋｃ１０２０、ＥＭＭ９００をはじめ、Ｋｃ配信用ＥＭＭやサーバ型放送方式のＴｙｐｅIIで用いられるＡＣＩ（Ａｃｃｏｕｎｔ　Ｃｏｎｔｒｏｌ　Ｉｎｆｏｒｍａｔｉｏｎ）などに設定するようにしても良い。また、ライセンス１６００に設定する情報を配信するのに加え、ライセンス１６００とは異なるフォーマットのライセンスを含めて配信するようにしても良いし、ＥＣＭやＥＭＭをライセンス１６００とは異なるフォーマットのライセンスであると考えることもできる。
【０２１６】
また、本発明における実施の形態では、ライセンス１６００をＩＣカード１０３内部に蓄積するようにしたが、ＩＣカード１０３の記憶容量が大きくない場合を考慮して、少なくともライセンス１６００の一部を端末装置１０２に蓄積するようにしても良い。この場合、ライセンス変換により生成したライセンス１６００のセキュリティを確保するために、暗号化が必要である。この暗号化においては、例えば、ＩＣカード１０３固有のマスタ鍵Ｋｍ２５２や複数の端末装置１０２であらかじめ共有している暗号鍵（グループ鍵）、あるいは、図１３で示した蓄積暗号鍵Ｋｍ’１３０３など、配信時のワーク鍵Ｋｗ２０３とは異なる暗号鍵を用いることにより、ライセンス１６００を端末装置１０２、ＩＣカード１０３や、これらの集合にバインドするようにしても良い。あるいは、ライセンス変換前のＫｃ伝送用ＥＣＭ１１００などを端末装置１０２の蓄積部１２０３にそのまま蓄積するようにしても良い。この際、暗号変換を行わずにそのまま蓄積しても良いし、ワーク鍵Ｋｗ２０３の定期的または不定期の更新に備えるため、ライセンス１６００と同様、Ｋｃ伝送用ＥＣＭの暗号変換を行うようにしても良い。なお、端末装置１０２およびＩＣカード１０３において、ライセンスの暗号変換処理を行う場合には、図２３に示すように、ＩＣカード１０３の内部にＥＣＭ／ＥＭＭ再暗号化部２３０１を追加すると良い。
【０２１７】
また、本発明における実施の形態では、ライセンス変換履歴であるＴＬ１５００において、ライセンスＩＤ１５０１を用いて、ライセンス変換を制御する場合の例を示したが、図２４に示すように、Ｋｃ伝送用ＥＣＭ２４００にＥＣＭを識別するためのＩＤ（ＥＣＭ－ＩＤ２４０１）を設けるようにしても良い。この場合、ＴＬ１５００において、ライセンスＩＤ１５０１に代えて、ＥＣＭ－ＩＤ２４０１を用いて、ライセンス変換を制御することができる。ただし、ライセンス１６００単位のライセンス変換制御ではなく、Ｋｃ伝送用ＥＣＭ１１００単位のライセンス変換制御となる。あるいは、ＴＬ１５００において、ライセンスＩＤ１５０１に加えて、ＥＣＭ－ＩＤ２４０１を合わせて用いることにより、ライセンス変換を制御するようにしても良い。この場合、異なるＫｃ伝送用ＥＣＭ１１

００に同一ライセンスＩＤのライセンス１６００が含まれるような場合（すなわち、異なるサービスから同一ライセンスを得る場合）や、通信ネットワーク１０５などから同一ライセンスＩＤのライセンス１６００を取得した場合でも、ライセンス１６００を取得した先を区別することができるため、異なるサービスから同一ライセンスを取得したい場合などにおいて、ライセンス変換ができないといった問題を解決することができる。さらに、これらのＩＤは、ライセンスやＫｃ伝送用ＥＣＭ１１００などを識別可能な情報であればこれに限られるものではないので、ライセンスのハッシュ値、ＭＡＣ、ＵＲＩなどを用いるようにしても良い。

【０２１８】

また、本発明における実施の形態では、Ｋｃ伝送用ＥＣＭ１１００のライセンス変換期限１１０６（ＴＬ１５００のライセンス変換期限１５０２）を絶対日時で表現したが、相対日時を設定するようにしても良い。例えば、ライセンス有効期限１１０８からの相対日時としても良いし、端末装置１０２でＫｃ伝送用ＥＣＭ１１００を受信した日時からの相対日時などとしても良い。また、変換が許可される終了日時のみである場合の例を示したが、合わせて開始日時を付与するようにしても良い。

【０２１９】

また、本発明における実施の形態では、ライセンス１６００には必ず有効期限１６０３が設定される場合の例を示したが、図２４で示したＫｃ伝送用ＥＣＭ２４００のように、有効期限１６０３（Ｋｃ伝送用ＥＣＭ２４００のライセンス有効期限１１０８）が無期限であり、Ｋｃ伝送用ＥＣＭ２４００にライセンス変換期限が設定されていない場合も考えられる。この場合には、ＩＣカード１０３のライセンス変換処理部１２１６がＴＬ１５００のライセンス変換期限１５０２を生成するようにしても良い。ライセンス変換期限１５０２の生成にあたっては、Ｋｃ伝送用ＥＣＭ２４００の受信日時やライセンス変換を行った日時に一定の期間（例えば、１ヶ月など）を加算するという方法などが考えられる。この加算値については、システム固定値として、端末装置１０２やＩＣカード１０３で保持しておく方法もあるが、デジタル放送１０４や通信ネットワーク１０５などで、放送局１０１から動的に変更できるようにしても良い。

【０２２０】

また、本発明における実施の形態では、ＴＬ１５００には、ライセンスＩＤ１５０１およびライセンス変換期限１５０２を記載する場合の例を示したが、図２５に示すように、ＴＬ２５００として、事業者ＩＤ２５０１、サービスタイプ２５０３、購入情報２５０４、取得ライセンス数２５０６を合わせて記載するようにしても良い。これによれば、事業者ＩＤ２５０１を記載するようにしているので、ライセンス２５０２を事業者毎にユニークな値とすることができる。また、サービスタイプ２５０３を記載するようにしているので、ティアコンテンツに関するライセンス変換履歴に加えて、ＰＰＶコンテンツに関するライセンス変換履歴も統合して管理することが可能となる。また、購入情報２５０４として、ＰＰＶコンテンツを購入した日時を合わせて記載するようにしている。また、取得ライセンス数２５０６を記載するようにしているので、あらかじめシステム固定値として設定されていたり、放送局１０１からＫｃ伝送用ＥＣＭ１１００などによって、１つのライセンスに関してユーザが取得可能なライセンス数（すなわち、コピー可能なライセンス数）が指定されたりする場合には、取得ライセンス数２５０６を記録することによって、取得可能なライセンス数を確実に制御することが可能となる。また、取得可能なライセンス数に限らず、それ以外のライセンスの取得に関する条件を管理するようにしても良い。

【０２２１】

なお、上記で説明したＴＬ２５００を用いる場合、サービスタイプ２５０３、購入情報２５０４を用いて、同一のＰＰＶコンテンツ（ＰＰＶライセンス）を再度購入する場合に、図２６に示すようなメッセージをユーザに提示することができる。

【０２２２】

図２６は、ユーザＩ／Ｆ部１２０８がユーザに提示するウォーニングメッセージの一例を示す図である。モニタ２６０１に表示されているメッセージ２６０２は、ユーザがコン

テンツ「神器２」のライセンスを２００４／４／１５　１９：００：００に購入済であるので、同一コンテンツを再購入してもよいか否かをユーザに確認する旨のメッセージを示している。

【０２２３】

なお、本発明における実施の形態では、ＩＣカード１０３で、最初にライセンス変換処理を行った端末装置１０２の端末装置ＩＤを記録しておくことにより、端末装置１０２とＩＣカード１０３とをバインドする場合の例を示したが、これに限られるものでなく、コンテンツやライセンスを共有可能な複数の端末装置１０２およびＩＣカード１０３からなるドメインと呼ばれる集合を識別するためのドメインＩＤを、端末装置ＩＤに代えて用いるようにしても良い。

【０２２４】

また、本発明における実施の形態では、ＴＬ１５００において、必ずライセンス変換期限１５０２を管理する場合の例を示したが、Ｋｃ伝送用ＥＣＭ１１００にライセンス変換期限１１０６やライセンス有効期限１１０８が設定されていないライセンスのライセンス変換履歴に関しては、時限で管理するのではなく、ＴＬ１５００のレコード数などにより管理し、古いレコードから消去するなど、ハイブリッドな構成とするようにしても良い。

【０２２５】

また、本発明における実施の形態では、Ｋｃ伝送用ＥＣＭ１１００のサービスタイプ１１０３を参照して、ＴＬ１５００にライセンス変換履歴のレコードを追加するか否かを決定するようにしたが、Ｋｃ伝送用ＥＣＭ１１００に設定されたコンテンツの利用条件（ライセンス有効期限１１０８、利用可能回数１１１０、書き出し可能回数１１１１などがあげられるが、これらに限られるものではない）がステートを有するか否かによって、レコードを追加するか否かを決定するようにしても良い。このため、Ｋｃ伝送用ＥＣＭ１１００またはライセンス１６００に、ステートを有するライセンスであるか否かの識別情報を設けても良い。例えば、利用条件がステートを有するライセンスのみレコードとして追加し、ステートを有さないライセンスはレコードとして追加しない、などの方法が考えられる。ここで、利用条件がステートを有するとは、主として利用可能回数１１１０、書き出し可能回数１１１１などの回数制限の利用条件などがあげられ、ステートを有さない利用条件としては、主として有効期限１１０８などがあげられる。

【０２２６】

また、本発明における実施の形態では、ＴＬ１５００において、新たなライセンス変換履歴のレコードを追加する際に、ライセンス変換期限１５０２が経過したレコードを削除するようにしたが、定期的にライセンス変換期限１５０２が経過したレコードを検索して、削除したり、ＩＣカード１０３が端末装置１０２から特定のコマンドを受信した場合に、ライセンス変換期限１５０２が経過したレコードを検索して、削除したりするようにしても良い。また、ライセンス変換期限１５０２が経過したレコードの削除のための条件を、放送局１０１から動的に更新できるようにしても良い。さらに、ユーザ指示によって削除させるようにしても良い。

【０２２７】

また、本発明における実施の形態では、ＩＣカード１０３の内部でＴＬ１５００を管理するようにしたが、ＩＣカード１０３の記憶容量を考慮して、少なくともＴＬ１５００の一部を端末装置１０２の蓄積部１２０３において保持するようにしても良い。このとき、蓄積部１２０３において、悪意あるユーザなどによるＴＬ１５００の不正な操作を防止するため、蓄積部１２０３に保持するＴＬ１５００のハッシュ値を、ＩＣカード１０３で保持する必要がある。また、この場合、ある端末装置１０２の蓄積部１２０３にＴＬ１５００を蓄積した場合、他の端末装置１０２で新たにライセンス取得（変換）を行うと、ユーザが取得可能なライセンス数の不整合が生ずる可能性がある。よって、端末装置１０２にＴＬ１５００を蓄積した場合には、当該端末装置１０２を一意に識別するＩＤをＩＣカード１０３で保持することにより、ライセンスを取得可能な端末装置１０２を限定する必要がある。また、事前にこのような問題を回避するため、最初にライセンスを取得した端末

装置１０２のＩＤをＩＣカード１０３で保持しておくことによって、あらかじめライセンスを取得可能な端末装置１０２を限定するようにしても良い。

【０２２８】

なお、上記のように、ライセンスを取得可能な端末装置１０２を限定する場合、図２７に示すように、「別端末で既にライセンスを取得しているため、この端末ではライセンスは取得できません。」などのメッセージ（２７０２）をユーザに提示するようにしても良い。合わせて、ライセンスを取得可能な端末の識別子（図２７では、ＴＥＲＭＩＮＡＬ－ＩＤ－１）を提示するようにしても良い。また、これに限らず、他のカードにライセンスを移動した場合などにメッセージをユーザに提示するようにしても良い。

【０２２９】

また、本発明における実施の形態では、ＩＣカード１０３単位でＴＬ１５００を管理するようにしたが、ＩＣカード１０３内部で放送局１０１（事業者）毎に管理するようにしても良い。また、複数のＩＣカード１０３間で連携することにより、複数ＩＣカード１０３（ドメイン）毎で管理するようにしても良い。

【０２３０】

また、ライセンス変換履歴であるＴＬ１５００を、放送局１０１や他の端末装置１０２、他のＩＣカード１０３に送信し、放送局１０１や他の端末装置１０２、他のＩＣカード１０３で利用することもできる。

【０２３１】

また、ＩＣカード１０３でのライセンス変換処理中において、端末装置１０２の電源断や、ＩＣカードの取り外しなどにより、ライセンス変換完了前にＴＬ１５００のみが残ってしまい、ユーザが不利益を被る場合に備えて、ＩＣカード１０３で一定の回数に限って再取得を許可するようにしたり、通信ネットワーク１０５を用いて、放送局１０１と通信を行い、ＴＬ１５００を参照しつつ、ライセンス１６００を再取得できるようにしたりすることもできる。

【０２３２】

また、本発明における実施の形態では、放送局１０１における送出装置、端末装置１０２を機能ブロックで構成することとしたが、図１７～図２２に示したフローチャートを実現するプログラムをＣＰＵ、記憶装置、通信装置などからなる汎用のコンピュータ装置で実行することによって、放送局１０１における送出装置や、端末装置１０２を実現するようにしてもよい。

【０２３３】

また、配信装置および端末装置を構成する各機能ブロックは、複数のシステムＬＳＩなどで実現してもよいし、単一のシステムＬＳＩで実現してもよい。

さらに、本発明における実施の形態では、単一の配信経路からコンテンツやライセンス、制御情報などを取得する場合の例を示したが、デジタル放送とインターネットを併用したり、パッケージメディアとインターネットを併用したりといった、複合的な配信経路から構成されたコンテンツ配信システムに適用することもできる。

【産業上の利用可能性】

【０２３４】

本発明にかかるデジタル権利管理システムは、端末装置で取得したライセンスＩＤと有効期限とを合わせてリストで管理し、少なくともライセンスの有効期限までレコードと保持することにより、不正なライセンス取得の防止と、管理するデータサイズの増大の防止とを両立できるという効果を有し、デジタル放送、デジタルＣＡＴＶ、インターネットなどによるコンテンツ配信サービスにおけるデジタル権利管理システムなどとして有用である。またパッケージメディアなどの可搬メディアなどによるコンテンツ配信サービスにおけるデジタル権利管理システムにも応用できる。

【図面の簡単な説明】

【０２３５】

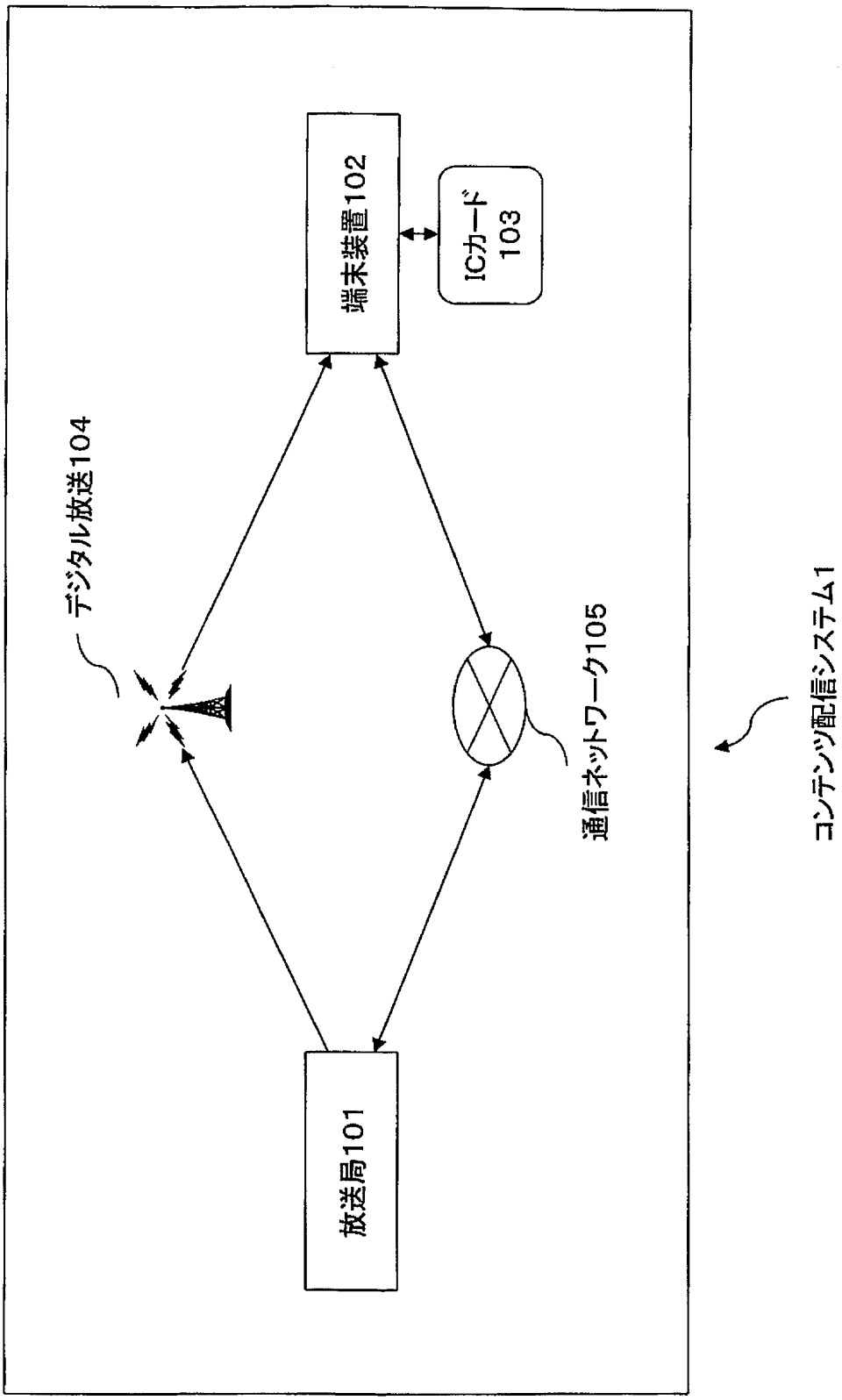
【図１】本発明の実施の形態に係るコンテンツ配信システム１の全体の概略構成を示

す図
【図２】本発明の実施の形態に係る暗号スキームの概要を示す図
【図３】本発明の実施の形態に係る放送局１０１の構成を示す機能ブロック図
【図４】本発明の実施の形態に係る契約情報管理ＤＢ３０１の契約情報管理テーブル４００の構成を示す図
【図５】本発明の実施の形態に係るワーク鍵ＤＢ３０２のワーク鍵管理テーブル５００の構成を示す図
【図６】本発明の実施の形態に係るコンテンツ属性情報ＤＢ３０３のコンテンツ属性情報管理テーブル６００の構成を示す図
【図７】本発明の実施の形態に係るコンテンツ鍵ＤＢ３０４のコンテンツ鍵管理テーブル７００の構成を示す図
【図８】本発明の実施の形態に係るコンテンツＤＢ３０５のコンテンツ管理テーブル８００の構成を示す図
【図９】本発明の実施の形態に係るＥＭＭ９００の構成を示す図
【図１０】本発明の実施の形態に係るＥＣＭ－Ｋｗ１０００、ＥＣＭ－Ｋｃ１０２０の構成を示す図
【図１１】本発明の実施の形態に係るＫｃ伝送用ＥＣＭ１１００の構成を示す図
【図１２】本発明の実施の形態に係る端末装置１０２の構成を示す図
【図１３】本発明の実施の形態に係るカード管理情報ＤＢ１２１０の共通情報テーブル１３００の構成を示す図
【図１４】本発明の実施の形態に係るカード管理情報ＤＢ１２１０の事業者別情報テーブル１４００の構成を示す図
【図１５】本発明の実施の形態に係るＴＬ１５００の構成を示す図
【図１６】本発明の実施の形態に係るライセンス１６００の構成を示す図
【図１７】本発明の実施の形態に係る放送局１０１における契約処理、端末装置１０２およびＩＣカード１０３におけるＥＭＭ受信処理を示すフローチャート
【図１８】本発明の実施の形態に係る放送局１０１におけるコンテンツ送出処理を示すフローチャート
【図１９】本発明の実施の形態に係る端末装置１０２およびＩＣカード１０３におけるコンテンツ蓄積処理を示すフローチャート
【図２０】本発明の実施の形態に係るライセンス変換不可時にユーザに提示するメッセージを示す図
【図２１】本発明の実施の形態に係るＩＣカード１０３におけるライセンス変換可否判定処理を示すフローチャート
【図２２】本発明の実施の形態に係る端末装置１０２およびＩＣカード１０３におけるコンテンツ利用処理を示すフローチャート
【図２３】本発明の実施の形態の変形例に係る端末装置１０２の構成を示す図
【図２４】本発明の実施の形態の変形例に係るＫｃ伝送用ＥＣＭ２４００の構成を示す図
【図２５】本発明の実施の形態の変形例に係るＴＬ２５００の構成を示す図
【図２６】本発明の実施の形態の変形例に係るＰＰＶコンテンツの重複購入検出時にユーザに提示するメッセージを示す図
【図２７】本発明の実施の形態の変形例に係る別端末でのライセンス取得済みによるライセンス取得不可時にユーザに提示するメッセージを示す図

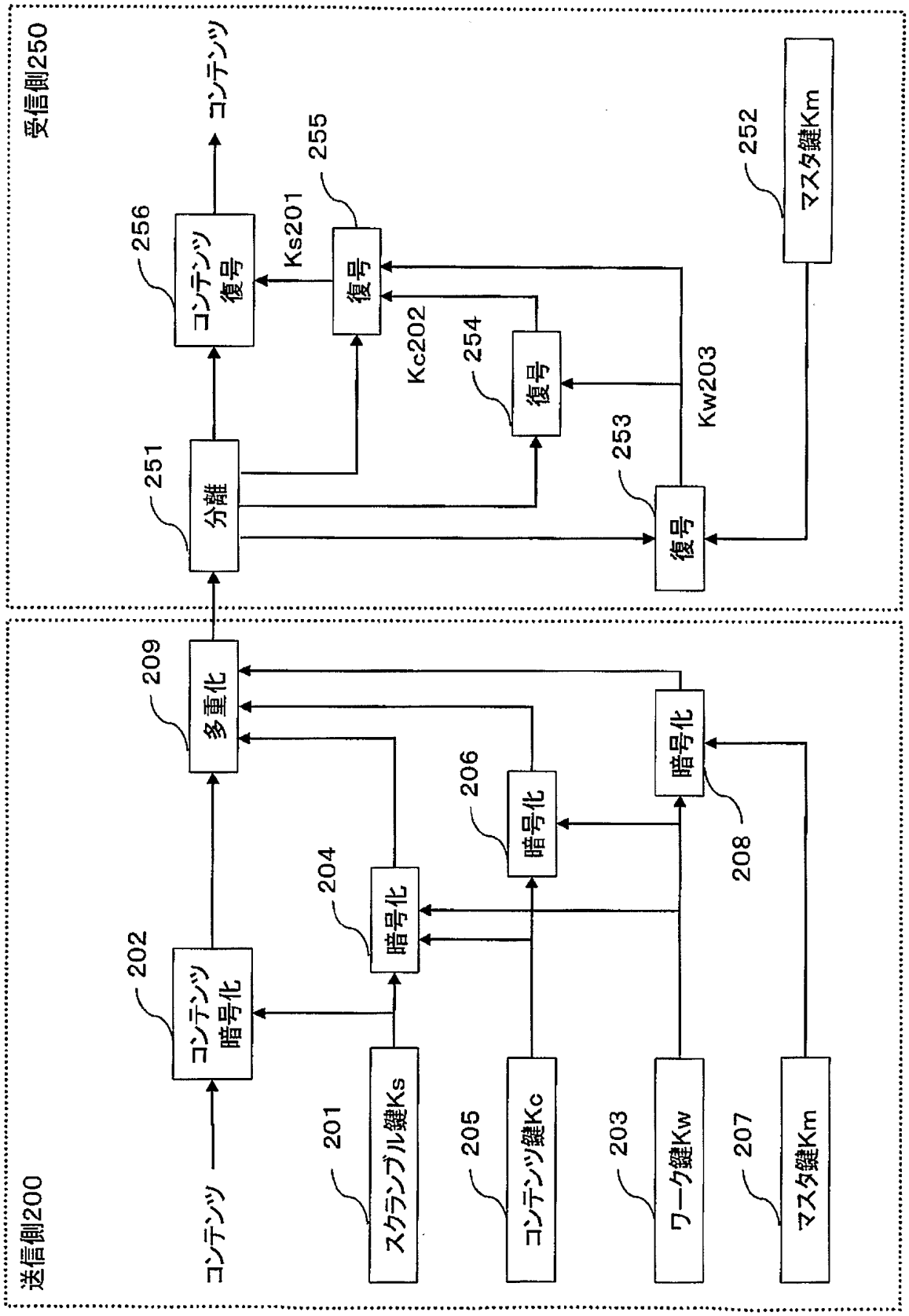
【符号の説明】
【０２３６】
１　コンテンツ配信システム
１０１　放送局
１０２　端末装置
１０３　ＩＣカード

１０４　デジタル放送
１０５　通信ネットワーク
２０１　スクランブル鍵Ｋｓ
２０３、５０２、１４０６　ワーク鍵Ｋｗ
２０５、７０３、１６０６　コンテンツ鍵Ｋｃ
２０７、２５２、４０６、１３０２　マスタ鍵Ｋｍ
３０１　契約情報管理ＤＢ
３０２　ワーク鍵ＤＢ
３０３　コンテンツ属性情報ＤＢ
３０４　コンテンツ鍵ＤＢ
３０５　コンテンツＤＢ
３０６　通信部
３０７　契約処理部
３０８　ＥＭＭ生成部
３０９　ＥＭＭ暗号化部
３１０　ＥＣＭ生成部
３１１　ＥＣＭ暗号化部
３１２　コンテンツ符号化部
３１３　多重化部
３１４　コンテンツ暗号化部
３１５　コンテンツ送出部
９００　ＥＭＭ
１０００　ＥＣＭ－Ｋｗ
１０２０　ＥＣＭ－Ｋｃ
１１００、２４００　Ｋｃ伝送用ＥＣＭ
１２０１　送受信部
１２０２　分離部
１２０３　蓄積部
１２０４　蓄積管理部
１２０５　コンテンツ復号部
１２０６　コンテンツ利用部
１２０７、１２１３　カードＩ／Ｆ部
１２０８　ユーザＩ／Ｆ部
１２１０　カード管理情報ＤＢ
１２１１　変換履歴ＤＢ
１２１２　ライセンスＤＢ
１２１４　ＥＣＭ／ＥＭＭ復号部
１２１５　ＥＣＭ／ＥＭＭ処理部
１２１６　ライセンス変換処理部
１２１７　ライセンス処理部
１５００、２５００　ＴＬ
１６００　ライセンス

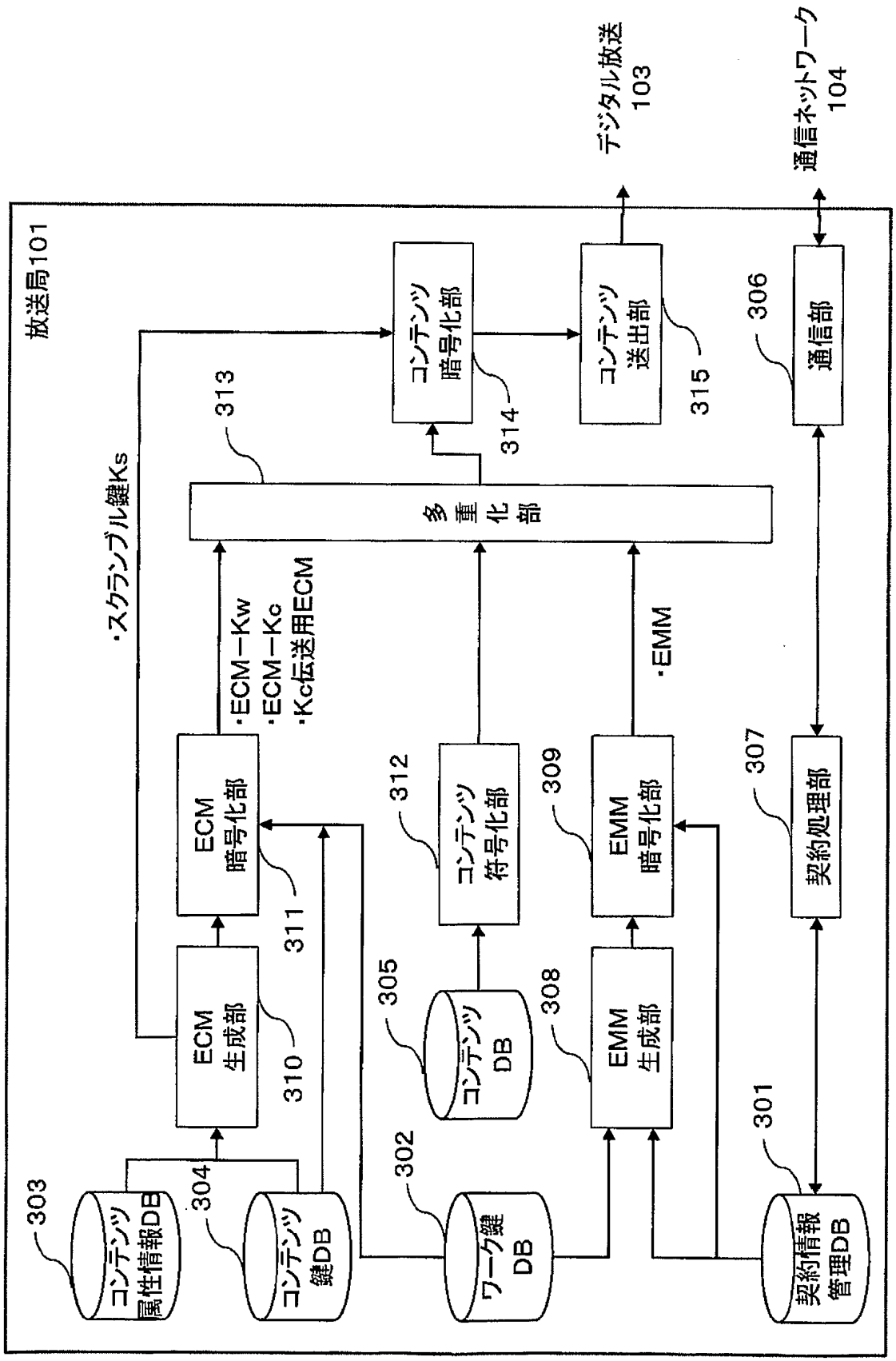
【書類名】図面
【図１】


端末装置102
ICカード
103
デジタル放送104
通信ネットワーク105
放送局101
コンテンツ配信システム1

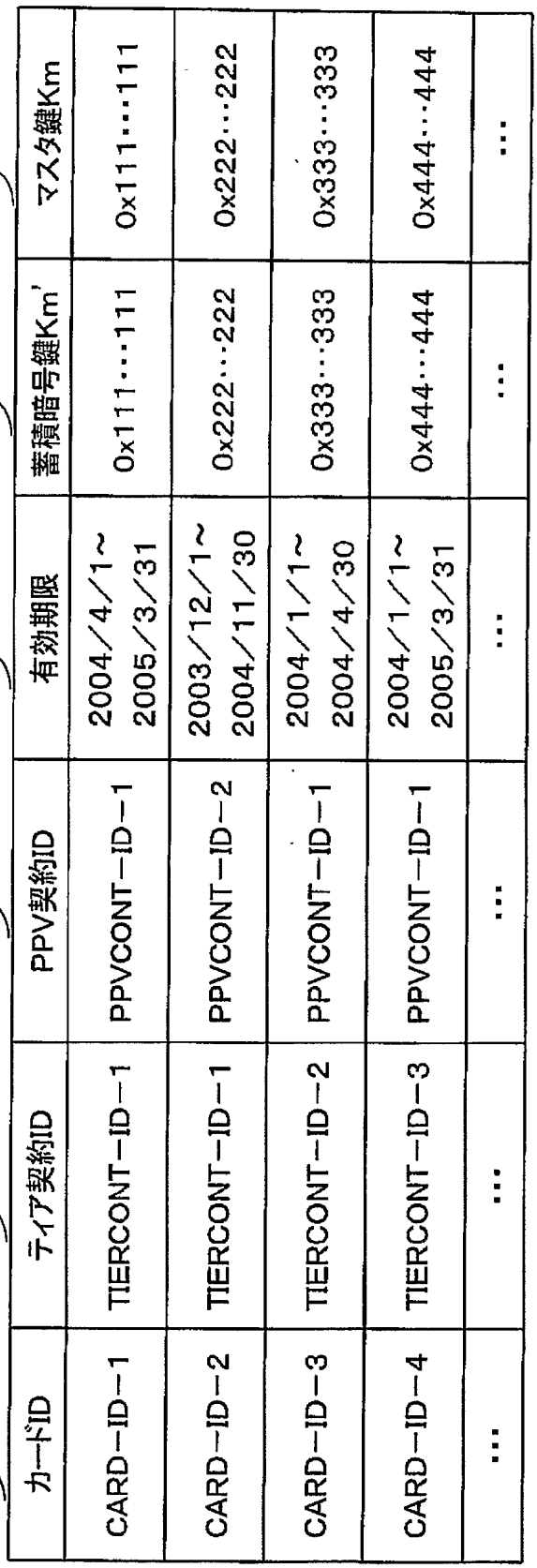
【図２】


送信側200
受信側250
コンテンツ
コンテンツ暗号化
202
スクランブル鍵Ks
201
暗号化
204
コンテンツ鍵Kc
205
暗号化
206
ワーク鍵Kw
203
暗号化
208
マスタ鍵Km
207
多重化
209
分離
251
コンテンツ復号
256
復号
255
Ks201
Kc202
復号
254
Kw203
復号
253
マスタ鍵Km
252
コンテンツ

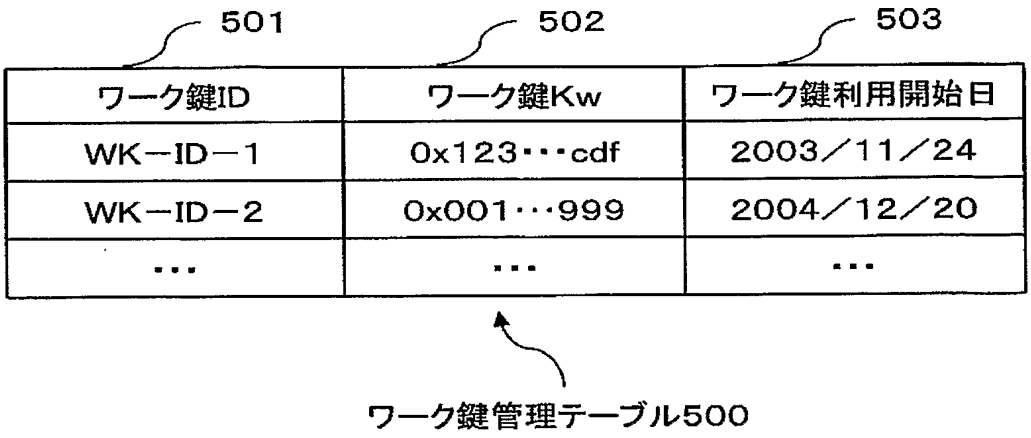
【図３】


放送局101
デジタル放送
103
通信ネットワーク
104
・スクランブル鍵Ks
・ECM－Kw
・ECM－Kc
・Kc伝送用ECM
・EMM
多重化部
313
コンテンツ暗号化部
314
コンテンツ送出部
315
通信部
306
ECM暗号化部
311
ECM生成部
310
コンテンツ符号化部
312
コンテンツDB
305
EMM暗号化部
309
EMM生成部
308
契約処理部
307
コンテンツ属性情報DB
303
コンテンツ鍵DB
304
ワーク鍵DB
302
契約情報管理DB
301

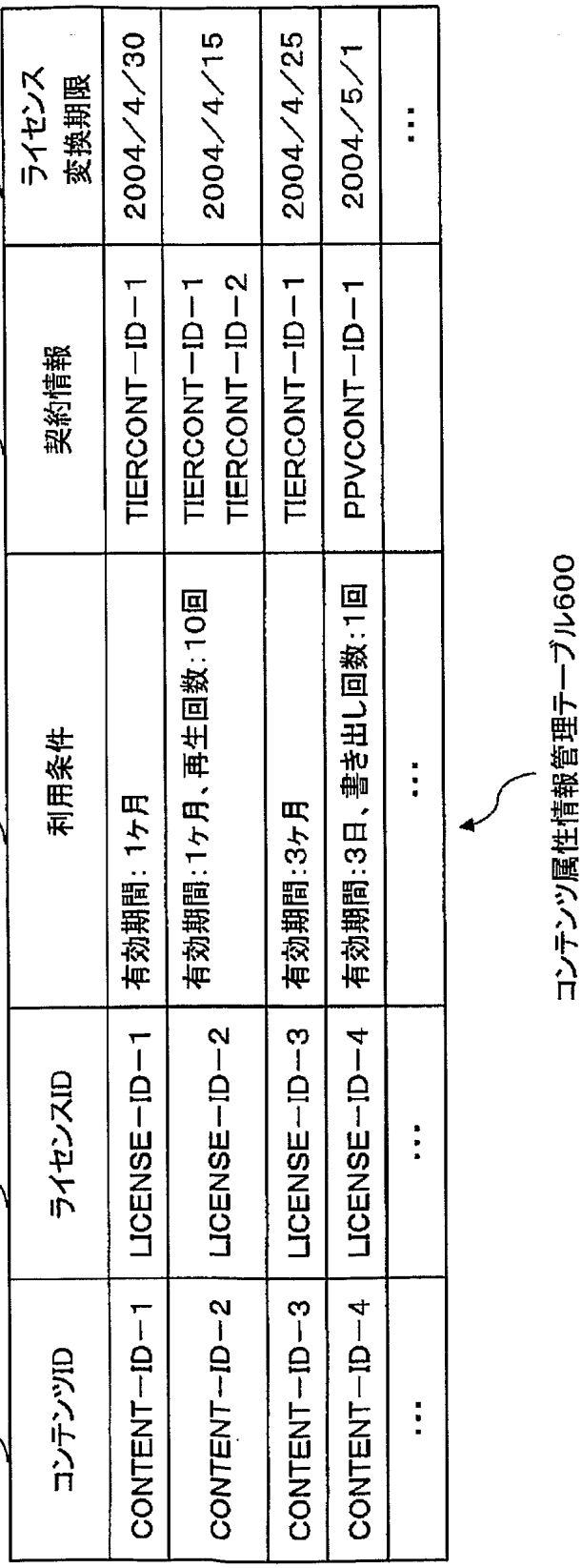
【図４】


401
402
403
404
405
406
カードID
ティア契約ID
PPV契約ID
有効期限
蓄積暗号鍵Km'
マスタ鍵Km
CARD－ID－1
TIERCONT－ID－1
PPVCONT－ID－1
2004／4／1～
2005／3／31
0x111…111
0x111…111
CARD－ID－2
TIERCONT－ID－1
PPVCONT－ID－2
2003／12／1～
2004／11／30
0x222…222
0x222…222
CARD－ID－3
TIERCONT－ID－2
PPVCONT－ID－1
2004／1／1～
2004／4／30
0x333…333
0x333…333
CARD－ID－4
TIERCONT－ID－3
PPVCONT－ID－1
2004／1／1～
2005／3／31
0x444…444
0x444…444
…
…
…
…
…
契約情報管理テーブル400

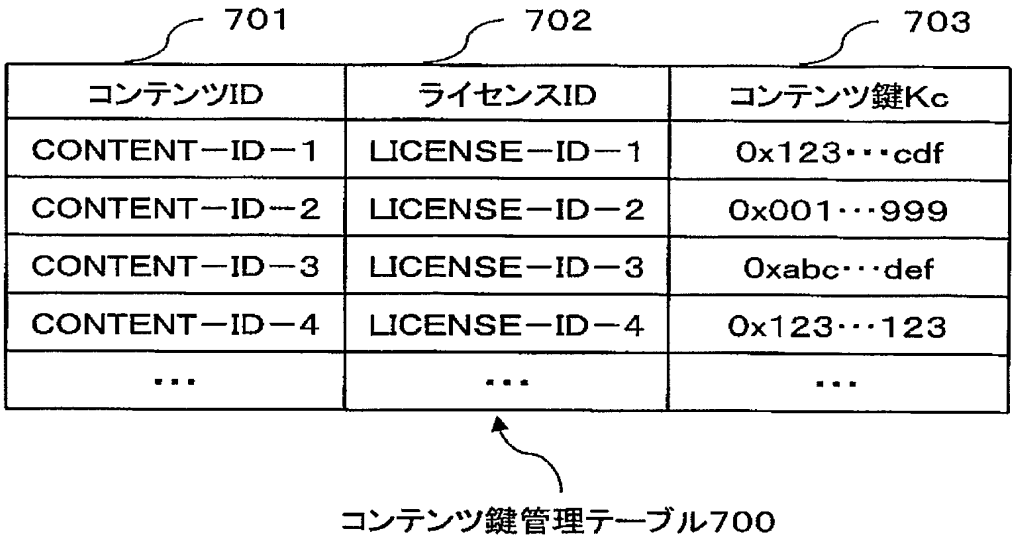
【図５】


501
502
503
ワーク鍵ID
ワーク鍵Kw
ワーク鍵利用開始日
WK－ID－1
0x123･･･cdf
2003／11／24
WK－ID－2
0x001･･･999
2004／12／20
･･･
･･･
･･･
ワーク鍵管理テーブル500

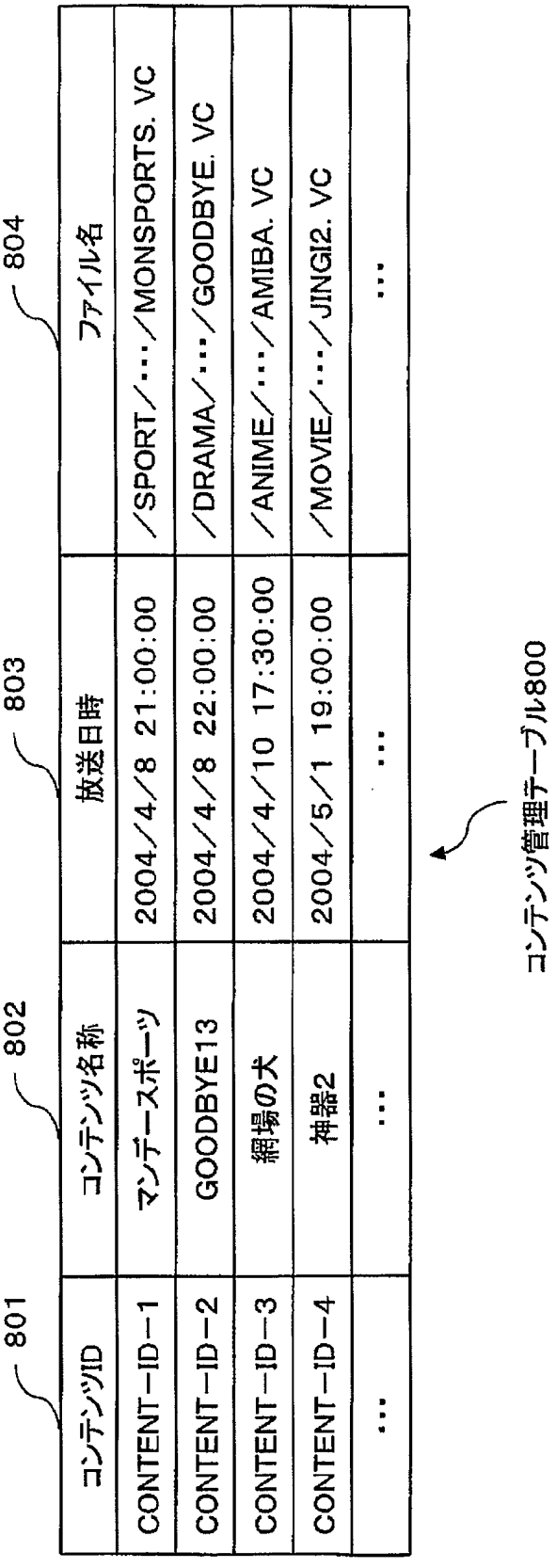
【図６】


601
602
603
604
605
コンテンツID
ライセンスID
利用条件
契約情報
ライセンス変換期限
CONTENT−ID−1
LICENSE−ID−1
有効期間：1ヶ月
TIERCONT−ID−1
2004／4／30
CONTENT−ID−2
LICENSE−ID−2
有効期間：1ヶ月、再生回数：10回
TIERCONT−ID−1
TIERCONT−ID−2
2004／4／15
CONTENT−ID−3
LICENSE−ID−3
有効期間：3ヶ月
TIERCONT−ID−1
2004／4／25
CONTENT−ID−4
LICENSE−ID−4
有効期間：3日、書き出し回数：1回
PPVCONT−ID−1
2004／5／1
…
…
…
…
コンテンツ属性情報管理テーブル600

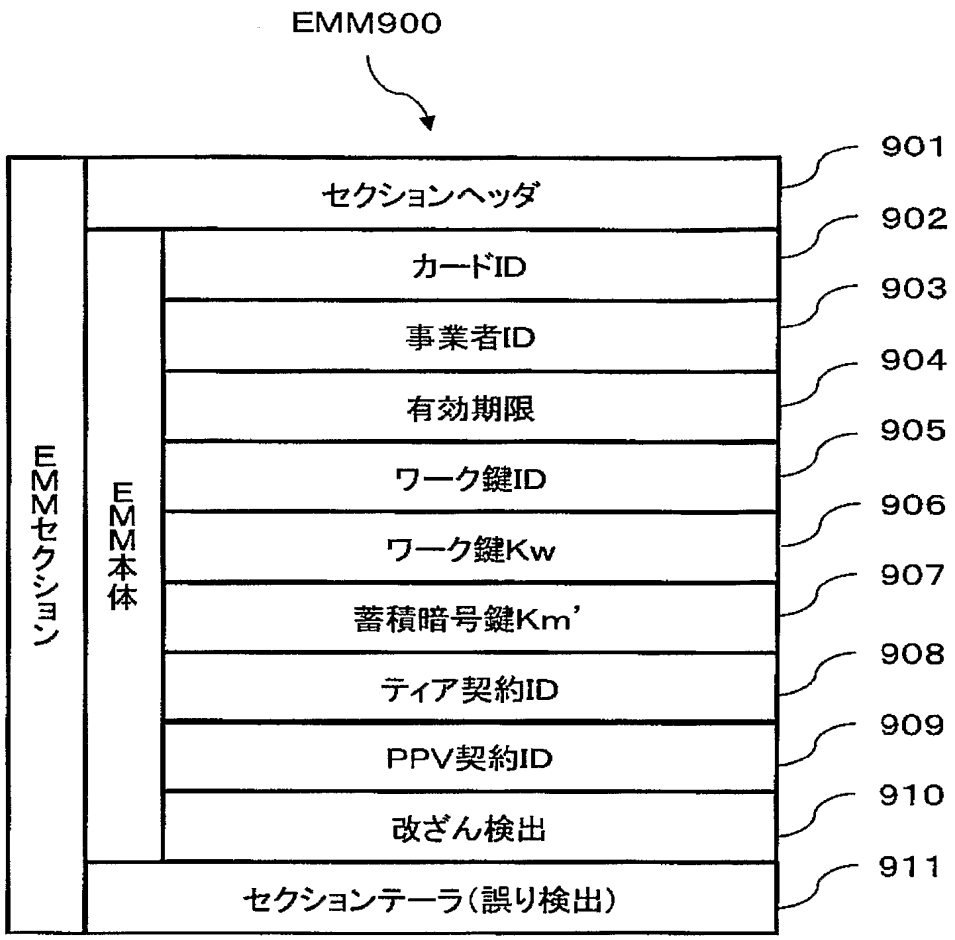
【図７】


701
702
703
コンテンツID
ライセンスID
コンテンツ鍵Kc
CONTENT－ID－1
LICENSE－ID－1
0x123･･･cdf
CONTENT－ID－2
LICENSE－ID－2
0x001･･･999
CONTENT－ID－3
LICENSE－ID－3
0xabc･･･def
CONTENT－ID－4
LICENSE－ID－4
0x123･･･123
･･･
･･･
･･･
コンテンツ鍵管理テーブル700

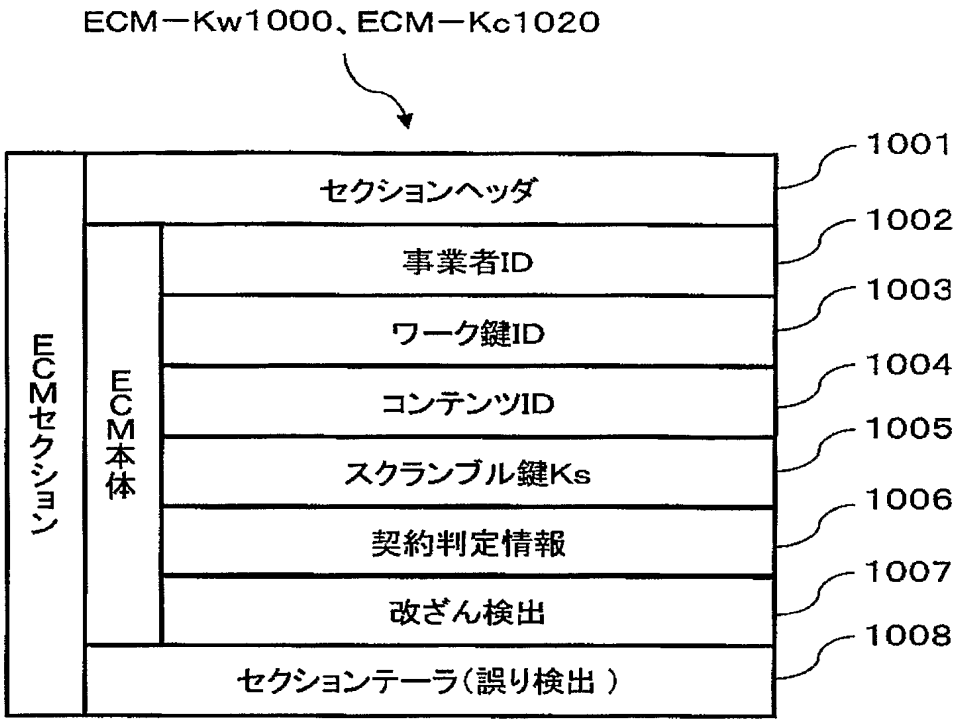
【図８】


801
802
803
804
コンテンツID
コンテンツ名称
放送日時
ファイル名
CONTENT－ID－1
マンデースポーツ
2004／4／8 21:00:00
／SPORT／・・・／MONSPORTS. VC
CONTENT－ID－2
GOODBYE13
2004／4／8 22:00:00
／DRAMA／・・・／GOODBYE. VC
CONTENT－ID－3
網場の犬
2004／4／10 17:30:00
／ANIME／・・・／AMIBA. VC
CONTENT－ID－4
神器2
2004／5／1 19:00:00
／MOVIE／・・・／JINGI2. VC
・・・
・・・
・・・
・・・
コンテンツ管理テーブル800

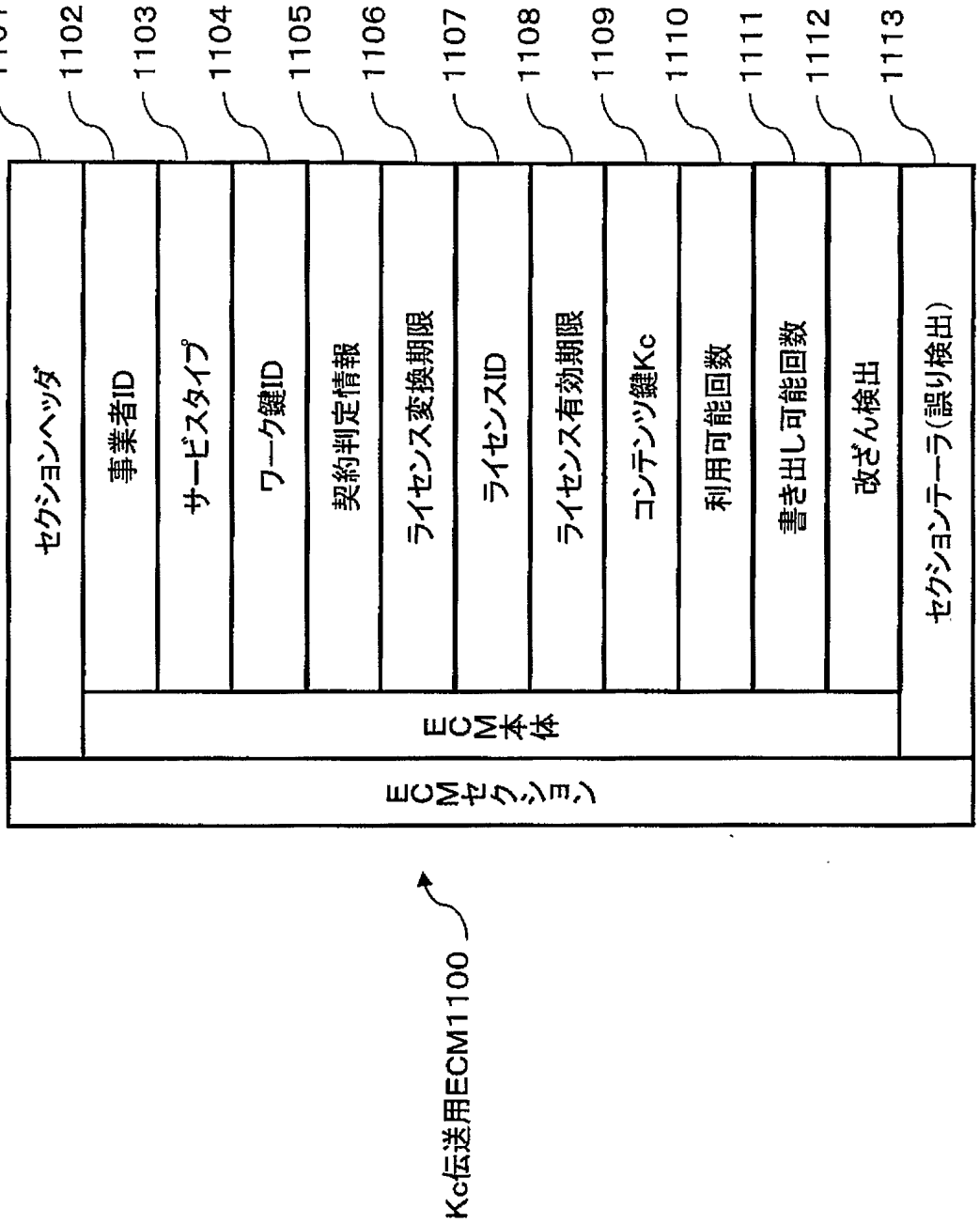
【図９】


EMM900
EMMセクション
EMM本体
セクションヘッダ
カードID
事業者ID
有効期限
ワーク鍵ID
ワーク鍵Kw
蓄積暗号鍵Km'
ティア契約ID
PPV契約ID
改ざん検出
セクションテーラ(誤り検出)
901
902
903
904
905
906
907
908
909
910
911

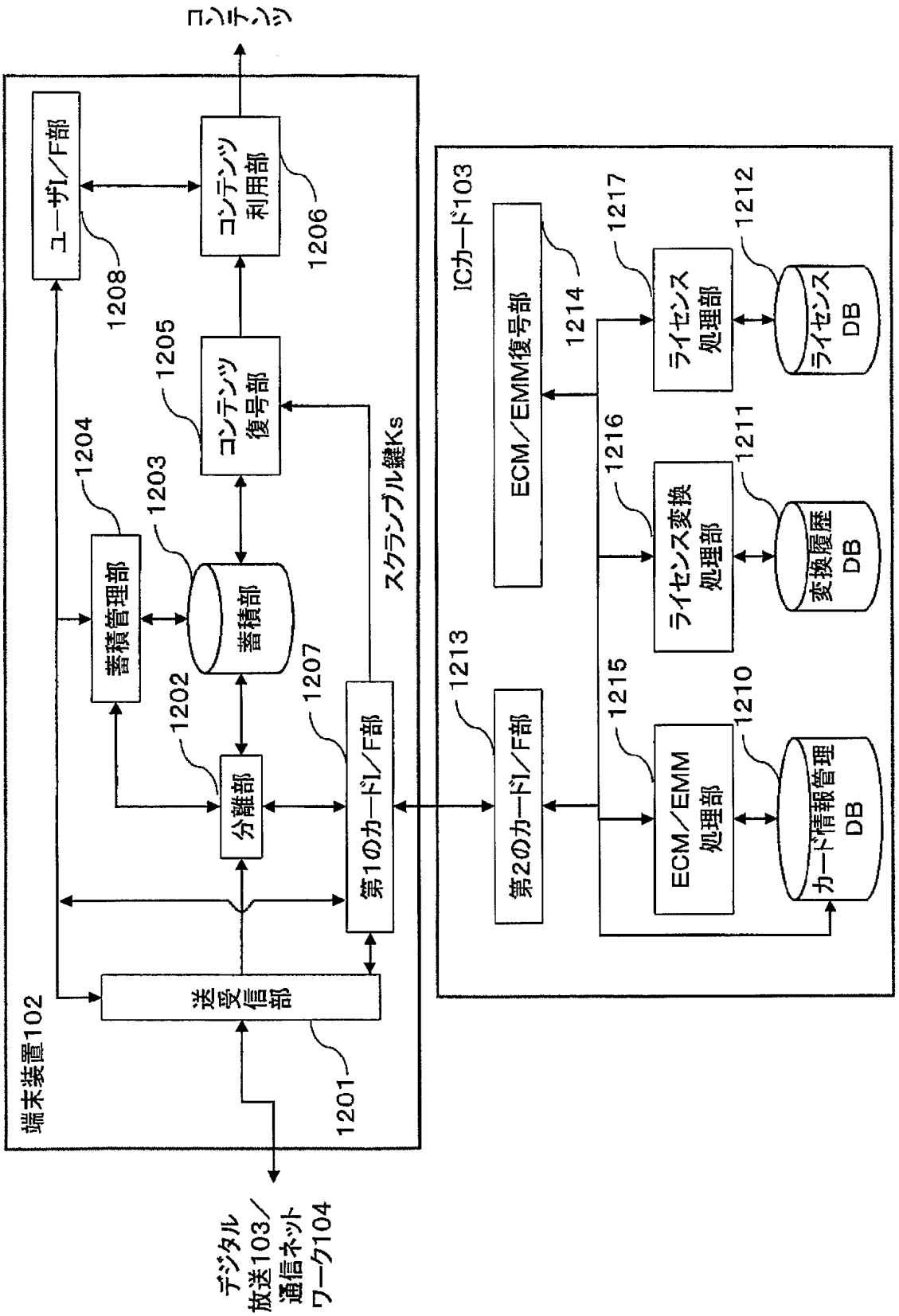
【図１０】


ECM－Kw1000、ECM－Kc1020
ECMセクション
ECM本体
セクションヘッダ
事業者ID
ワーク鍵ID
コンテンツID
スクランブル鍵Ks
契約判定情報
改ざん検出
セクションテーラ（誤り検出）
1001
1002
1003
1004
1005
1006
1007
1008

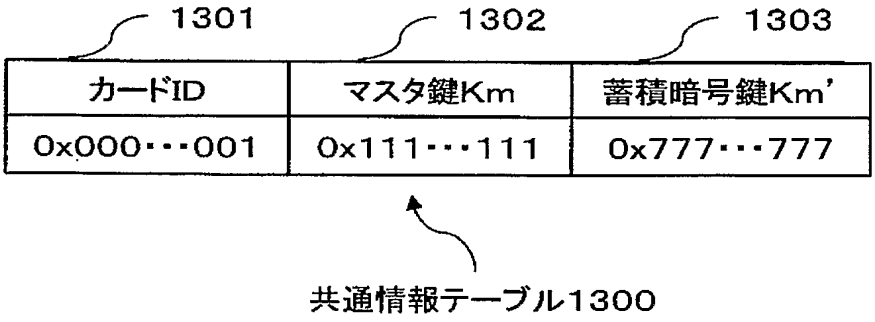
【図１１】


1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
セクションヘッダ
事業者ID
サービスタイプ
ワーク鍵ID
契約判定情報
ライセンス変換期限
ライセンスID
ライセンス有効期限
コンテンツ鍵Kc
利用可能回数
書き出し可能回数
改ざん検出
セクションデータ(誤り検出)
ECM本体
ECMセクション
Kc伝送用ECM1100

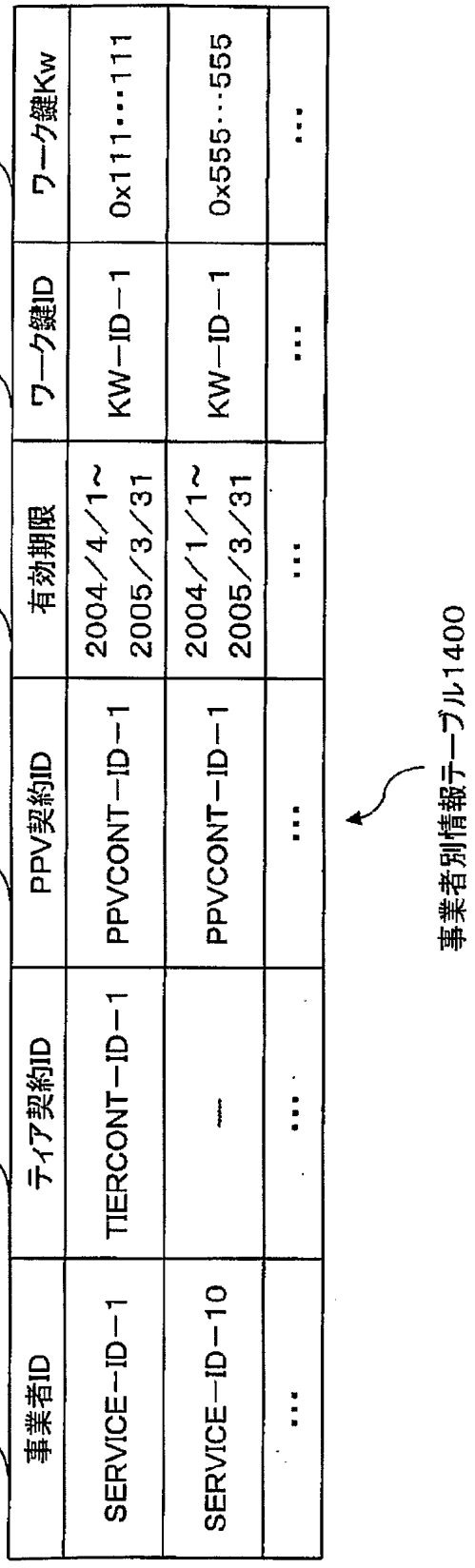
【図１２】


コンテンツ
端末装置102
ユーザI／F部
1208
コンテンツ利用部
1206
コンテンツ復号部
1205
蓄積管理部
1204
蓄積部
1203
分離部
1202
第1のカードI／F部
1207
スクランブル鍵Ks
送受信部
1201
デジタル放送103／通信ネットワーク104
ICカード103
ECM／EMM復号部
1214
第2のカードI／F部
1213
ライセンス処理部
1217
ライセンスDB
1212
ライセンス変換処理部
1216
変換履歴DB
1211
ECM／EMM処理部
1215
カード情報管理DB
1210

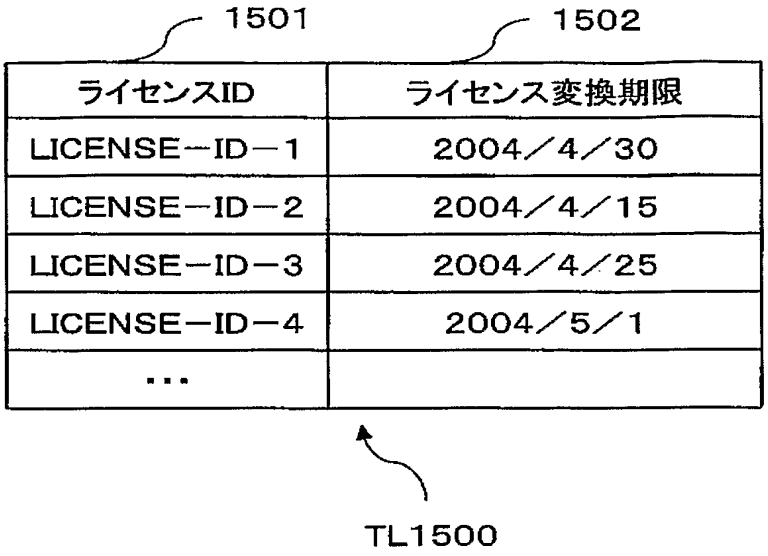
【図１３】


1301
1302
1303
カードID
マスタ鍵Km
蓄積暗号鍵Km'
0x000･･･001
0x111･･･111
0x777･･･777
共通情報テーブル1300

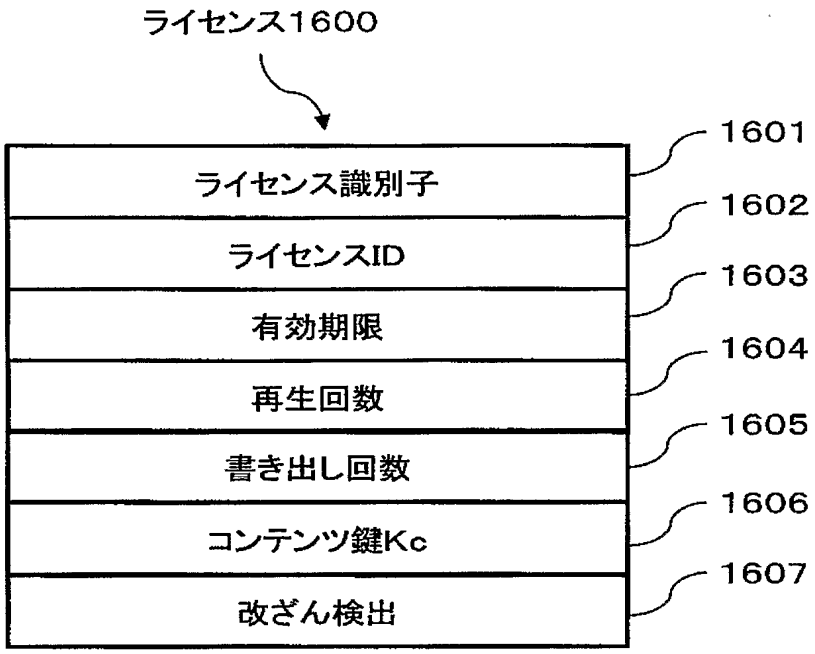
【図１４】


1401
1402
1403
1404
1405
1406
事業者ID
ティア契約ID
PPV契約ID
有効期限
ワーク鍵ID
ワーク鍵Kw
SERVICE－ID－1
TIERCONT－ID－1
PPVCONT－ID－1
2004／4／1～
2005／3／31
KW－ID－1
0x111･･･111
SERVICE－ID－10
―
PPVCONT－ID－1
2004／1／1～
2005／3／31
KW－ID－1
0x555･･･555
･･･
･･･
･･･
･･･
･･･
事業者別情報テーブル1400

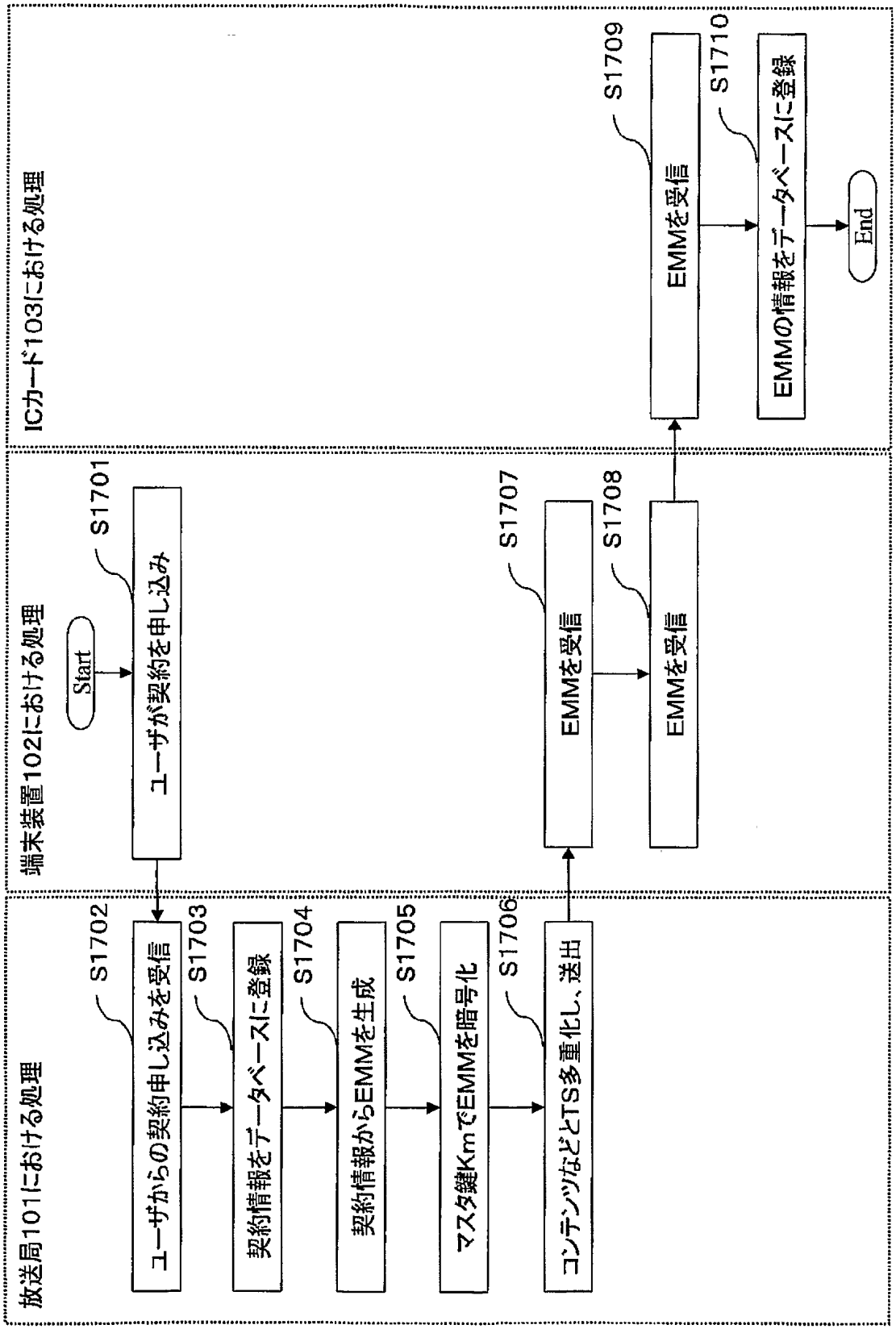
【図１５】


1501
1502
ライセンスID
ライセンス変換期限
LICENSE－ID－1
2004／4／30
LICENSE－ID－2
2004／4／15
LICENSE－ID－3
2004／4／25
LICENSE－ID－4
2004／5／1
・・・
TL1500

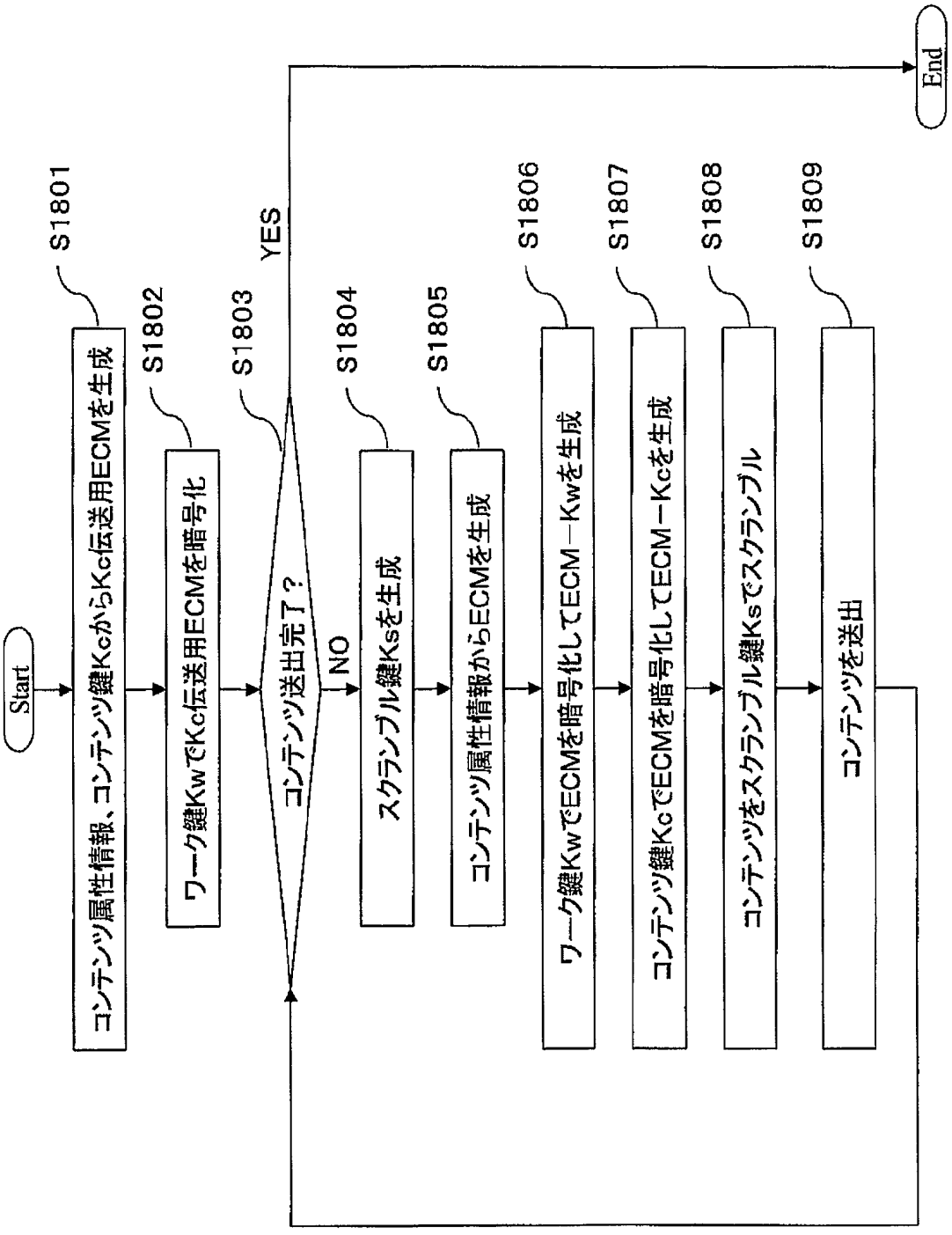
【図１６】


ライセンス1600
ライセンス識別子
ライセンスID
有効期限
再生回数
書き出し回数
コンテンツ鍵Kc
改ざん検出
1601
1602
1603
1604
1605
1606
1607

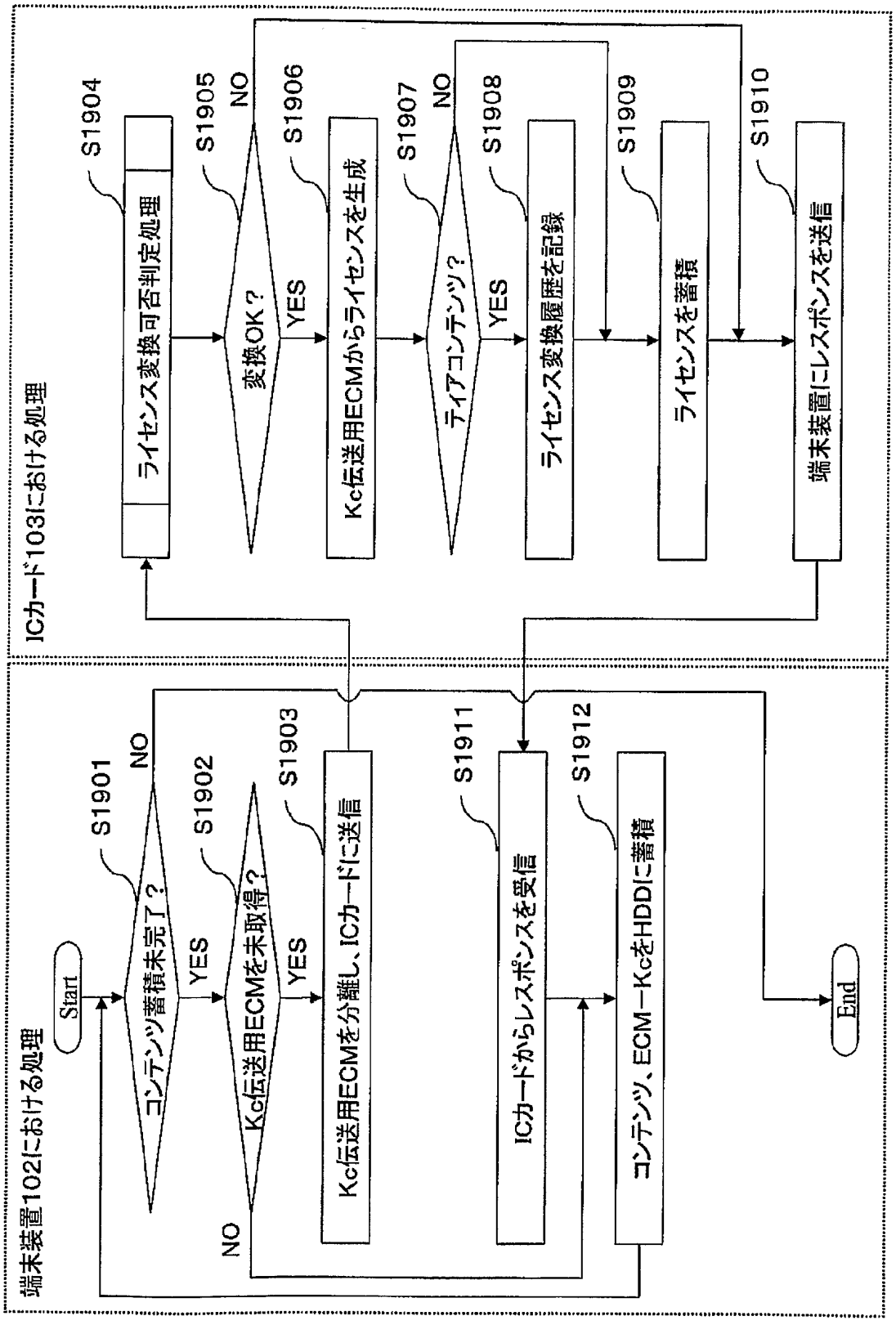
【図１７】


ICカード103における処理
端末装置102における処理
放送局101における処理
Start
S1701
ユーザが契約を申し込み
S1702
ユーザからの契約申し込みを受信
S1703
契約情報をデータベースに登録
S1704
契約情報からEMMを生成
S1705
マスタ鍵KmでEMMを暗号化
S1706
コンテンツなどとTS多重化し、送出
S1707
EMMを受信
S1708
EMMを受信
S1709
EMMを受信
S1710
EMMの情報をデータベースに登録
End

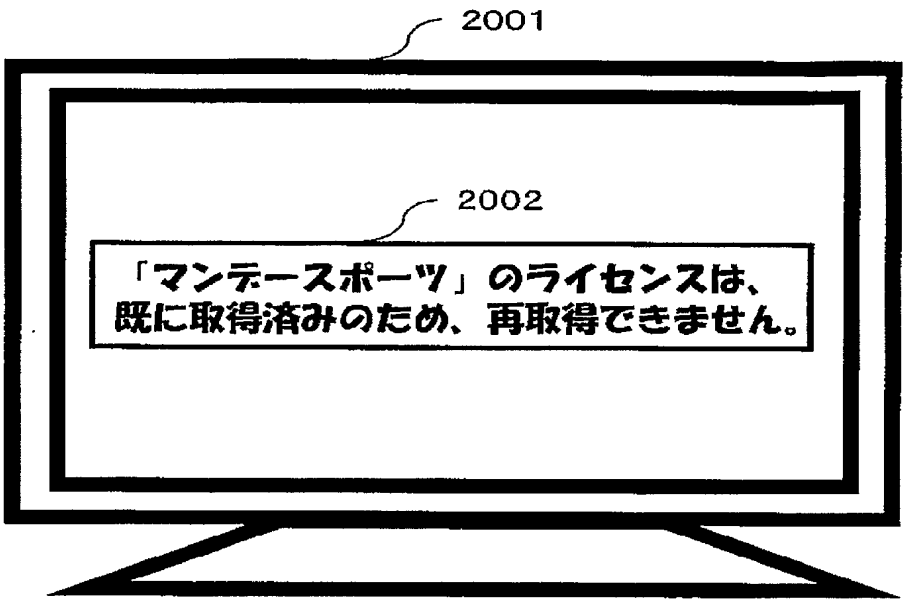
【図１８】


Start
S1801
コンテンツ属性情報、コンテンツ鍵KcからKc伝送用ECMを生成
S1802
ワーク鍵KwでKc伝送用ECMを暗号化
S1803
コンテンツ送出完了？
YES
NO
S1804
スクランブル鍵Ksを生成
S1805
コンテンツ属性情報からECMを生成
S1806
ワーク鍵KwでECMを暗号化してECM－Kwを生成
S1807
コンテンツ鍵KcでECMを暗号化してECM－Kcを生成
S1808
コンテンツをスクランブル鍵Ksでスクランブル
S1809
コンテンツを送出
End

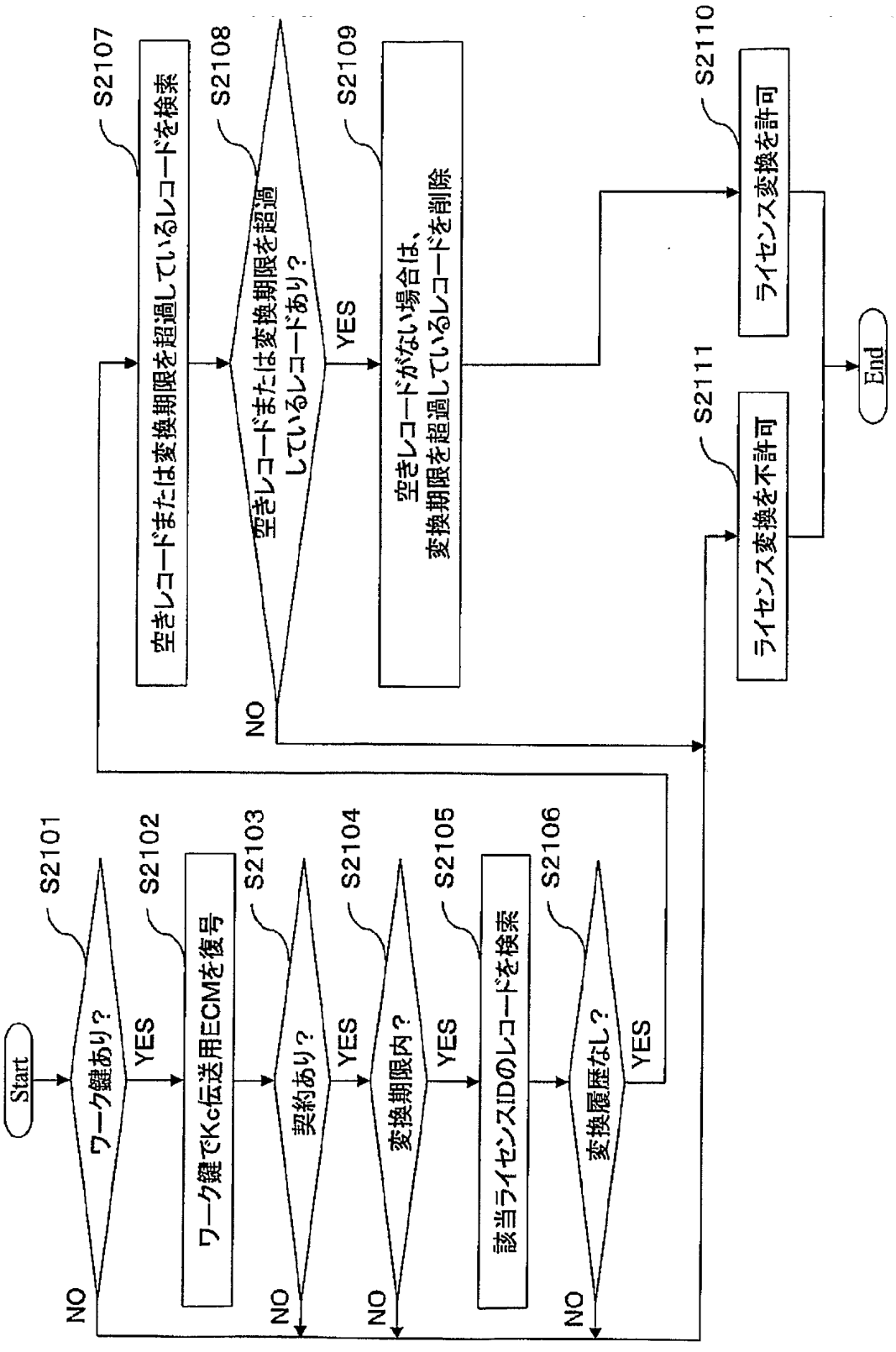
【図１９】


ICカード103における処理
S1904
ライセンス変換可否判定処理
S1905
変換OK？
NO
YES
S1906
Kc伝送用ECMからライセンスを生成
S1907
テイアコンテンツ？
NO
YES
S1908
ライセンス変換履歴を記録
S1909
ライセンスを蓄積
S1910
端末装置にレスポンスを送信
端末装置102における処理
Start
S1901
コンテンツ蓄積未完了？
NO
YES
S1902
Kc伝送用ECMを未取得？
NO
YES
S1903
Kc伝送用ECMを分離し、ICカードに送信
S1911
ICカードからレスポンスを受信
S1912
コンテンツ、ECM－KcをHDDに蓄積
End

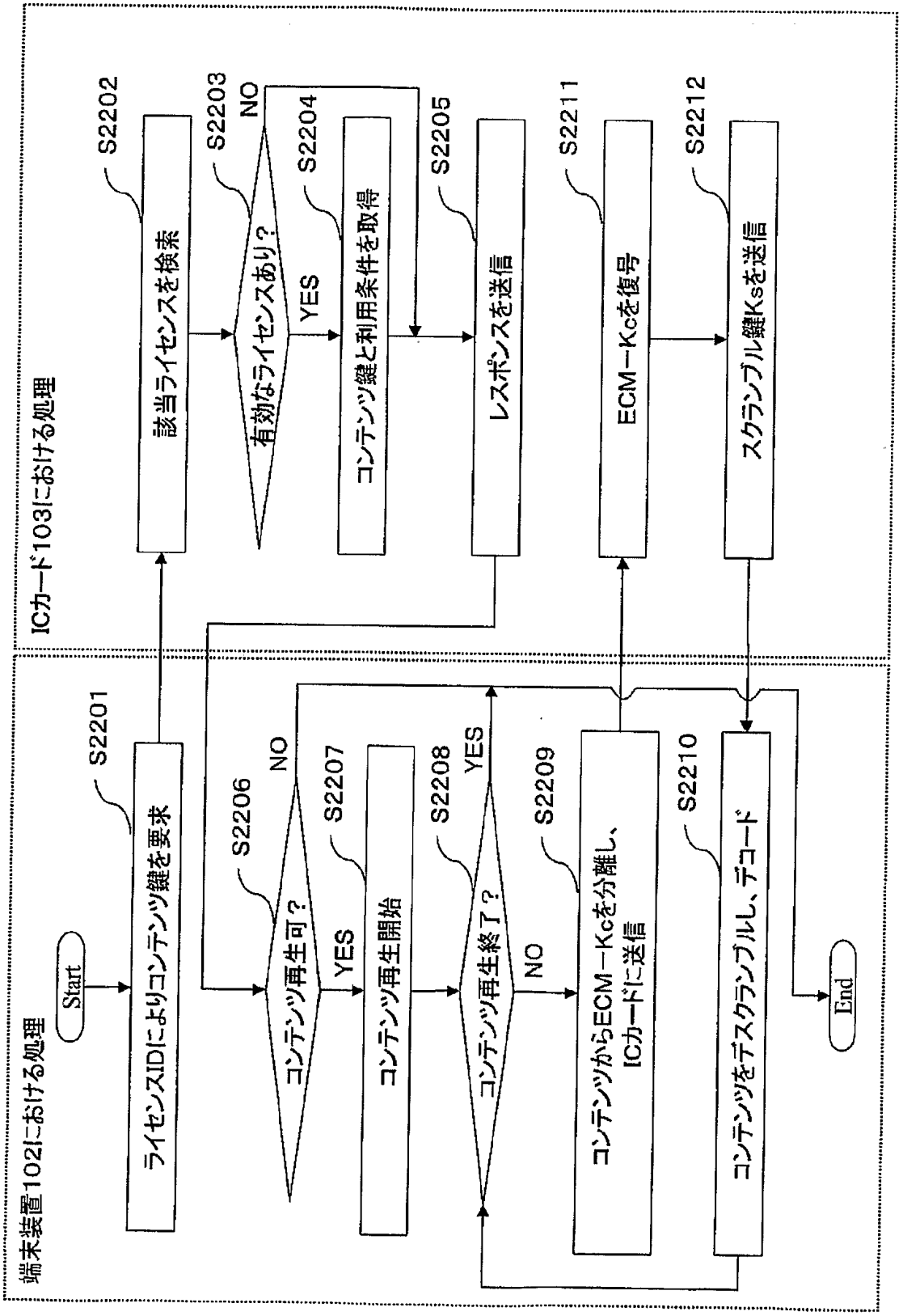
【図２０】



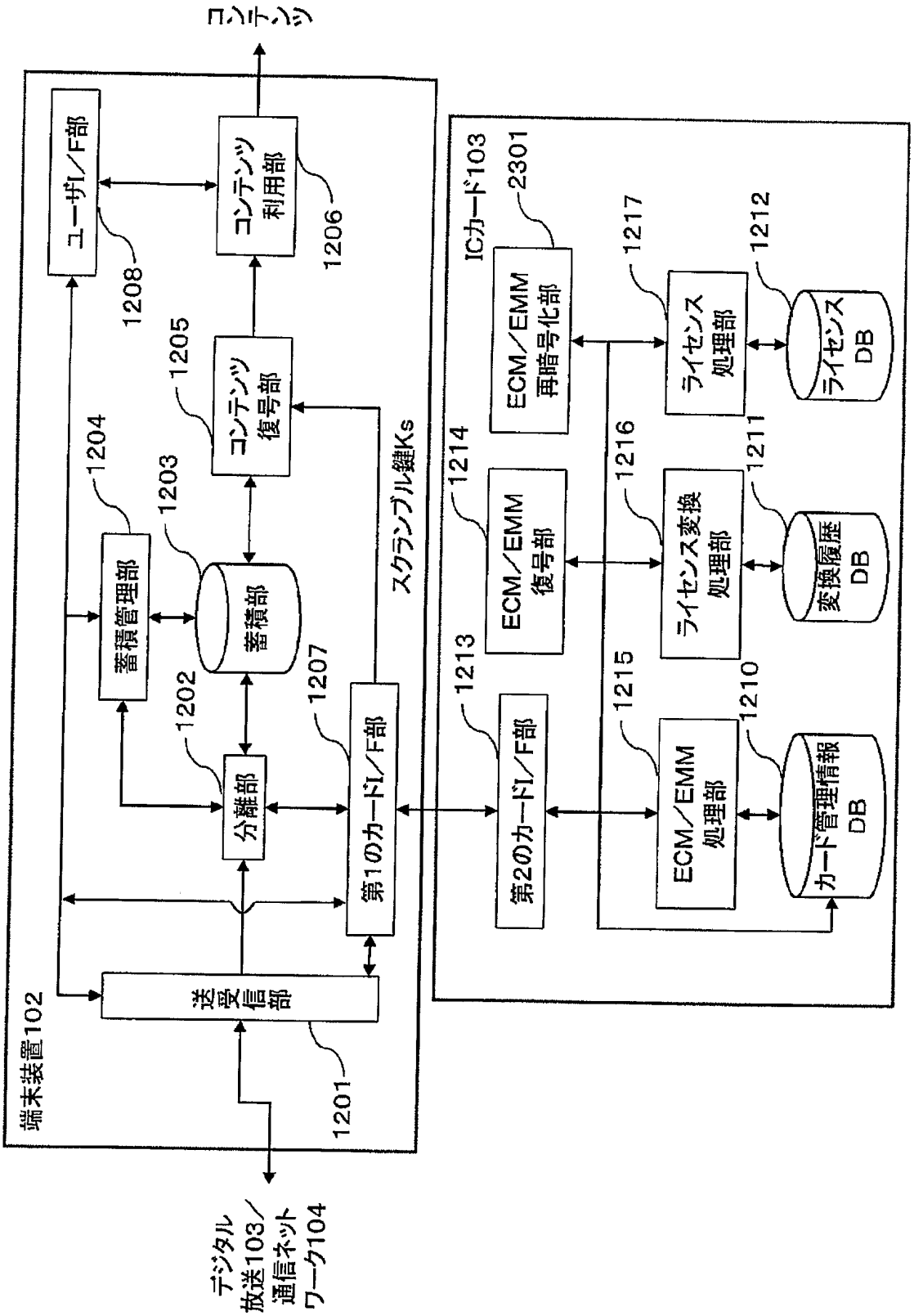
【図２１】


Start
S2101
ワーク鍵あり？
NO
YES
S2102
ワーク鍵でKc伝送用ECMを復号
S2103
契約あり？
NO
YES
S2104
変換期限内？
NO
YES
S2105
該当ライセンスIDのレコードを検索
S2106
変換履歴なし？
NO
YES
S2107
空きレコードまたは変換期限を超過しているレコードを検索
S2108
空きレコードまたは変換期限を超過
しているレコードあり？
NO
YES
S2109
空きレコードがない場合は、
変換期限を超過しているレコードを削除
S2110
ライセンス変換を許可
S2111
ライセンス変換を不許可
End

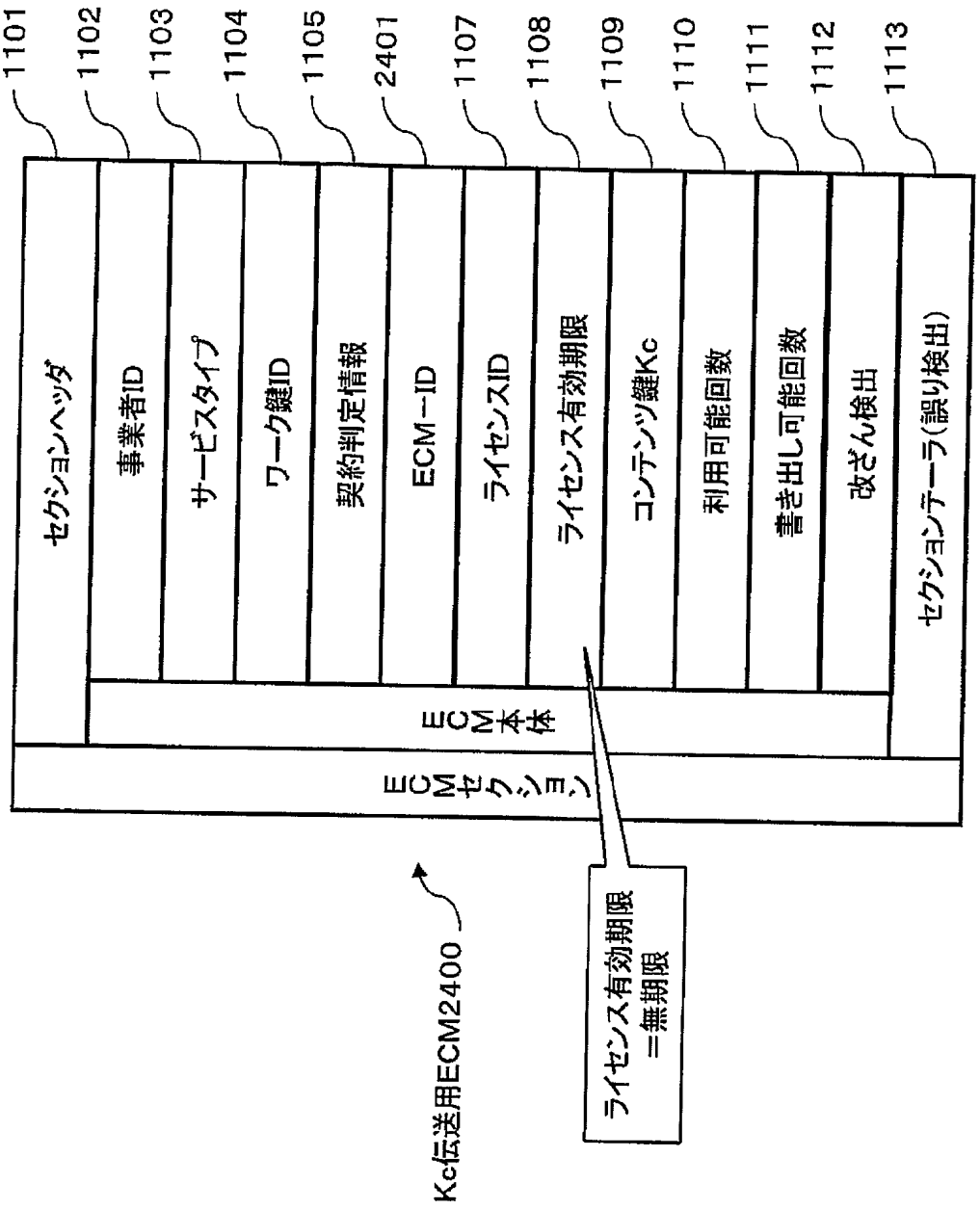
【図２２】


端末装置102における処理
ICカード103における処理
Start
S2201
ライセンスIDによりコンテンツ鍵を要求
S2202
該当ライセンスを検索
S2203
有効なライセンスあり？
NO
YES
S2204
コンテンツ鍵と利用条件を取得
S2205
レスポンスを送信
S2206
コンテンツ再生可？
NO
YES
S2207
コンテンツ再生開始
S2208
コンテンツ再生終了？
YES
NO
S2209
コンテンツからECM－Kcを分離し、ICカードに送信
S2210
コンテンツをデスクランブルし、デコード
End
S2211
ECM－Kcを復号
S2212
スクランブル鍵Ksを送信

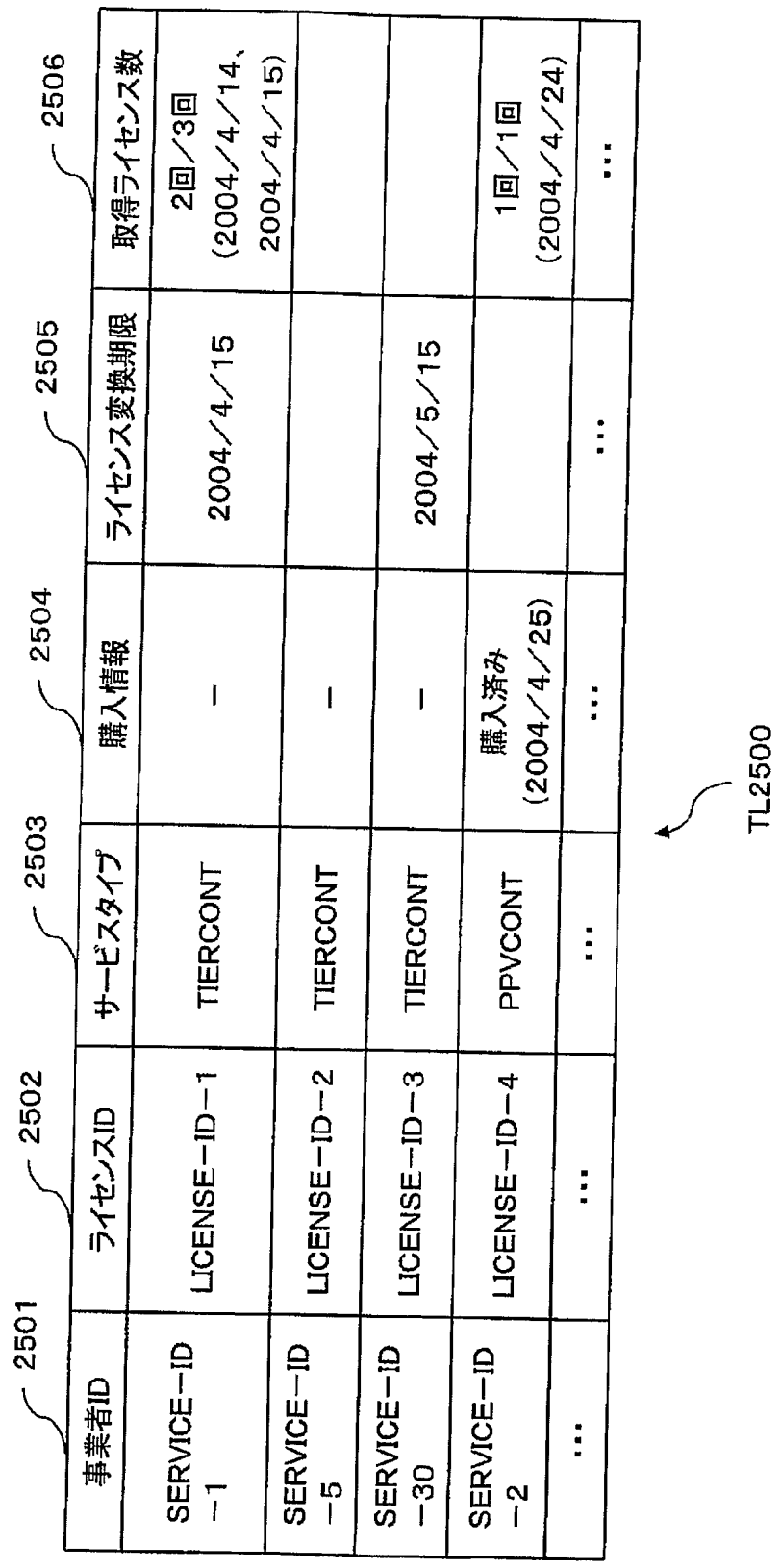
【図２３】


コンテンツ
端末装置102
ユーザI／F部
1208
コンテンツ利用部
1206
コンテンツ復号部
1205
蓄積管理部
1204
蓄積部
1203
分離部
1202
第1のカードI／F部
1207
スクランブル鍵Ks
送受信部
1201
デジタル放送103／通信ネットワーク104
ICカード103
2301
ECM／EMM再暗号化部
1217
ライセンス処理部
1212
ライセンスDB
1214
ECM／EMM復号部
1216
ライセンス変換処理部
1211
変換履歴DB
1213
第2のカードI／F部
1215
ECM／EMM処理部
1210
カード管理情報DB

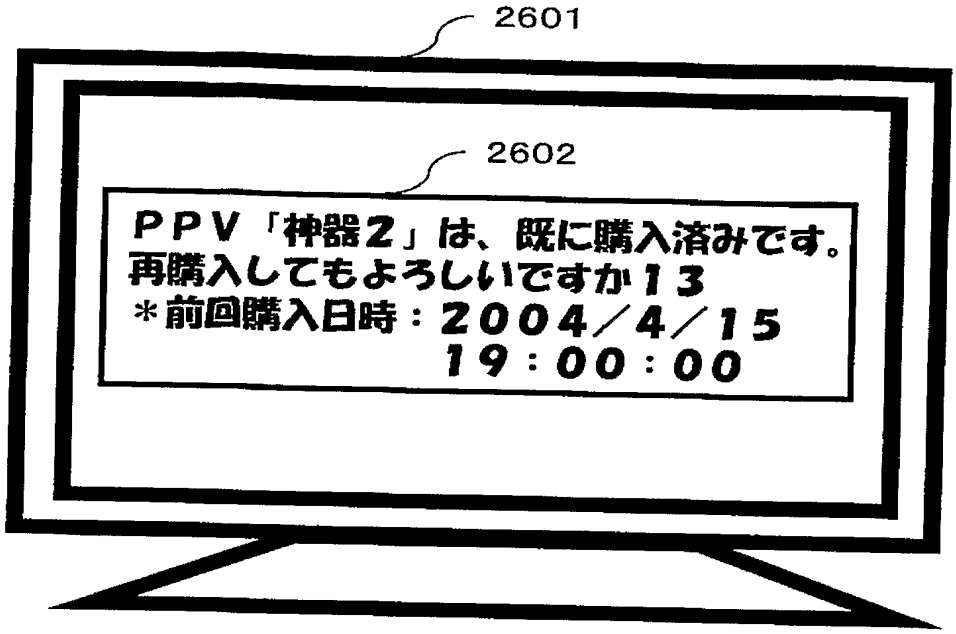
【図２４】


1101
1102
1103
1104
1105
2401
1107
1108
1109
1110
1111
1112
1113
セクションヘッダ
事業者ID
サービスタイプ
ワーク鍵ID
契約判定情報
ECM−ID
ライセンスID
ライセンス有効期限
コンテンツ鍵Kc
利用可能回数
書き出し可能回数
改ざん検出
セクションテーラ(誤り検出)
ECM本体
ECMセクション
Kc伝送用ECM2400
ライセンス有効期限
=無期限

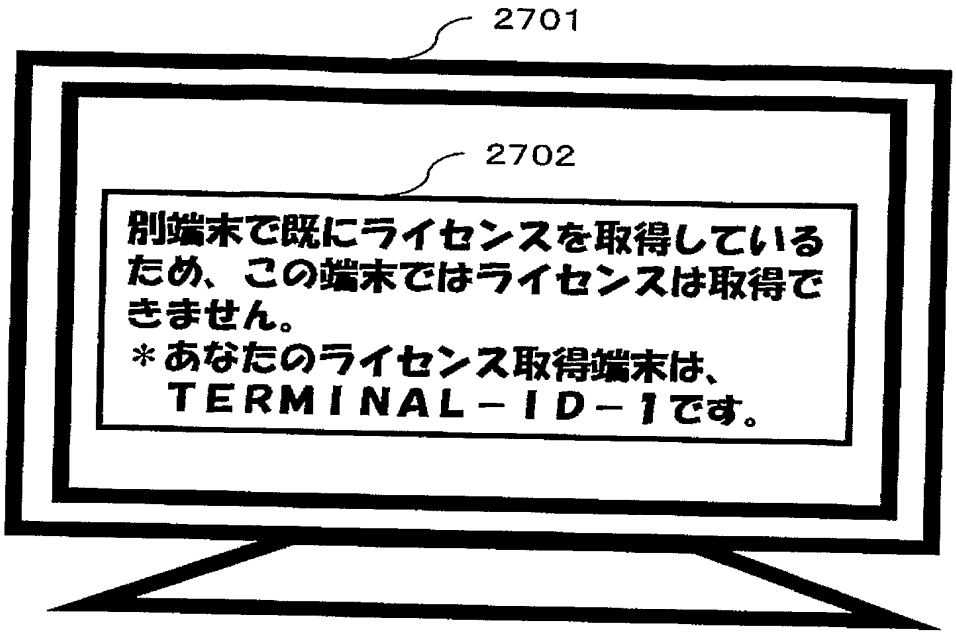
【図２５】


2501
2502
2503
2504
2505
2506
事業者ID
ライセンスID
サービスタイプ
購入情報
ライセンス変換期限
取得ライセンス数
SERVICE－ID－1
LICENSE－ID－1
TIERCONT
－
2004／4／15
2回／3回（2004／4／14、2004／4／15）
SERVICE－ID－5
LICENSE－ID－2
TIERCONT
－
SERVICE－ID－30
LICENSE－ID－3
TIERCONT
－
2004／5／15
SERVICE－ID－2
LICENSE－ID－4
PPVCONT
購入済み（2004／4／25）
1回／1回（2004／4／24）
…
…
…
…
TL2500

【図２６】


2601
2602
ＰＰＶ「神器２」は、既に購入済みです。
再購入してもよろしいですか１３
＊前回購入日時：２００４／４／１５
１９：００：００

【図２７】


2701
2702
別端末で既にライセンスを取得しているため、この端末ではライセンスは取得できません。
＊あなたのライセンス取得端末は、
ＴＥＲＭＩＮＡＬ－ＩＤ－１です。

【書類名】要約書
【要約】
【課題】　デジタル放送で配信するライセンスの不正取得を抑制し、事業者の権利を保護可能なデジタル権利管理システムを提供する。
【解決手段】　送出装置は、生成するライセンスにＩＤとライセンス取得期限を付与し、端末装置は、ライセンスに付加されたライセンスＩＤとライセンス取得期限とを含むライセンス取得履歴を記録する。端末装置は、ライセンスの取得時に既に同一ライセンスを取得している場合は、ライセンスの取得を抑制する。また、ライセンス取得履歴記録手段は、少なくともライセンス取得期限まで保持する。
【選択図】　図１２

認定・付加情報

特許出願の番号	特願２００４－１０６３３９
受付番号	５０４００５４７３１４
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１６年　４月　１日

＜認定情報・付加情報＞

【提出日】　平成16年 3月31日

特願２００４－１０６３３９

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社